

U.S. AIR FORCE
Project RAND

RECOMMENDATION

TO THE AIR STAFF

DEVELOPMENT OF THE DISTRIBUTED
ADAPTIVE MESSAGE-BLOCK NETWORK

August 30, 1965

Attachments:

1. Rand recommendation.
2. Letter from the Air Force.
3. Chapter by Paul Baran from recent book on packet switching that discusses rationale for each feature of packet switching and how it came about.
4. P-1995.
5. Calendar pages.
6. IEEE Spectrum Aug. 1964, p. 114.
7. List of RAND depository libraries.

RAND

30 August 1965

L-17930

Deputy Chief of Staff, Research and Development
Headquarters, United States Air Force
Washington, D. C. 20330

SUBJECT: DEVELOPMENT OF THE DISTRIBUTED ADAPTIVE MESSAGE-BLOCK
NETWORK

SUMMARY

We have reached an appropriate point in our work on "distributed networks" to recommend to the Air Force a specific direction of development.

I wrote to you on this subject on August 24, 1964 (L-17082) and General Curtin forwarded a request on December 23, 1964 for evaluation of the eleven RAND Memoranda by AFSC (and RTD, ESD, Lincoln), AFLC, (and GEEIA), and AFCS. Detailed comments were received and forwarded to RAND. A series of briefings and discussions ensued. Some technical difficulties were revealed, but these appear to be correctable with minor changes in the proposed system. A RAND Memorandum describing these adjustments is in preparation.

In our view it is possible to build a new large common-user communication network able to withstand heavy damage. Such a network can provide a major step forward in Air Force military communication capability. Although there can be no certainty of success because of the complex nature of the required development, the high potential pay-off leads us to recommend that the research and development portions of the following program be undertaken now. We can now purchase an option on lead time at minimum cost. If the research is successful, we will be in a position to move rapidly into implementation of the full network. Only after the preliminary engineering has been completed will there be sufficient information to determine precisely where and how much of such a network should be built.

Deputy Chief of Staff,
Research and Development

-2-

30 August 1965

Although the system is a marked departure from the existing communication system, we believe that after the R and D is proved out the new system can be integrated with the present one on an incremental basis.

We will be happy to help in any way as the program evolves. A further discussion of the problem and the proposed solution is attached.

Sincerely,

ORIGINAL SIGNED BY
F. R. COLLBOHM

F. R. Collbohm

Attachment: Limitations of Present Networks and the Improvements We Seek

ATTACHMENT

LIMITATIONS OF PRESENT NETWORKS AND THE IMPROVEMENTS WE SEEK

- * 1. Most communication networks are highly vulnerable to overt and covert attack. A new, large, highly-interconnected distributed network, shared among all military users would offer a major improvement in survivability. (See ODC I.)*
- 2. Most military communication is transmitted with negligible protection against loss of critical information to an eavesdropper. Only a small portion of the total military communication load is cryptographically protected. The military is often highly constrained in subjects that it can discuss over the telephone for fear of eavesdropping. The universal availability of secure communications will be helpful to those having need to transmit classified information. (See ODC IX.)
- 3. Today, those who connect computers to other computers and to the remote entry devices used in command and control systems are not satisfied with the high error rate of a communication network which was not originally designed for digital transmission. Computers can be intolerant of errors caused by the communication links. The use of automatic error correction features could help achieve the desired, almost error-free user-to-user performance--less than one error in 100 million transmitted bits. (See ODC VI through VIII.)
- 4. Partially because of high cost, military "hard copy" (paper) traffic is primarily limited to center-to-center operation. This produces long delay times between end users. A system that will reduce the cost of digital transmission will help make hard copy facilities more widespread at the action officer level. (See ODC V and VIII.)

* ODC is an abbreviation for "On Distributed Communications," the series of memoranda described in Appendix.

5. We lack complete flexibility of connection between users where secrecy is mandatory. We desire a system in which it will be possible to speak quickly to anyone, anywhere without prior arrangement for the communications. (See ODC VIII and IX.)
6. Military communication volume is increasing rapidly, and greater efficiency would result from better user-to-user communications. We want a system better able to handle larger volumes of traffic than commonly experienced today. Better military effectiveness could result if communications were not treated as a scarce resource that must be highly rationed. (See ODC V and VIII.)
7. Because of the difficulty in assigning costs to communications in the military, it is difficult to determine exactly how much we are presently paying. Estimates range from one-half to three billion dollars annually, with this cost increasing about 15 percent annually. In the belief that markedly more military communication is indicated in the future, it becomes mandatory to lay the groundwork upon which to build future communication networks that achieve the desired long range demand for digital and voice communications at minimum cost. The maturity of digital technology allows us to think broadly and differently regarding communications. The concept of an all digital communications network (as opposed to the traditional analog communication networks) allows the designer and user great freedom in survivability, flexibility, growth, secure communications and in handling the expected exponential growth in the transmission of digital data. (See ODC X.).

HOW THE PROPOSED NETWORK DIFFERS FROM PRESENT DAY NETWORKS

The proposed network is described in detail in the ODC series of RAND Memoranda. Some of the key differences between it and the present concepts of building communication networks are:

- ★ 1. Use of digital techniques in lieu of analog circuits throughout the entire network, both in transmission and in switching.

2. Cryptographic techniques designed as an integral portion of the switching mechanism to provide secrecy for all network users--whether transmitting classified traffic or not.
- * 3. The communication network designed as a "bit-transportation system," rather than a "real-time" connection of a series of links.
- * 4. Integral automatic error detection and repeat (via a different route) transmission to allow the use of low cost and unreliable links in the network.
- * 5. Adaptive routing for high user reliability during peak load periods including enemy attacks.
- * 6. Provisions to allow each user to "carry his telephone number" with him.

SPECIFIC RECOMMENDATIONS

We recommend that a research and development program be undertaken which can lead eventually to the construction and implementation of the Distributed Adaptive Message-Block Network described in the referenced RAND Memoranda.

- [We recommend that only the research and development phases be undertaken at this time,] with further implementation to follow the successful completion of the preliminary work phases.

- * [Because of the complex nature of the undertaking and the intricacy of the sub-systems, an unusual high level and continuity of technical expertise in digital technology is required in the development and its system management. We suggest that the research and development tasks be divided into separate contracts, each portion awarded to an organization particularly competent within its own field. This division by task imposes stringent technical competence on the system manager. To aid in this complex and technically difficult effort, we feel that a technical advisory panel should be constituted to review on-going study and development contracts and insure that necessary technical liaison and interaction among the various sub-contractors take place.

- * [Because much of the proposed system is based on digital computer techniques, organizations with demonstrated experience in the computer field will probably bring greater pertinent competence to bear in key aspects of the system development than organizations experienced only in traditional analog communication practices.]

DEVELOPMENT COST AND RATE

While no definite time-money expenditure rates are enumerated, the order of magnitude of the effort is described in Volume XI of the ODC series. Possibly five million dollars would be an appropriate amount for the initiation of this development effort.

We are not presuming to outline the detailed sequence of actions that might be taken. We have, however, prepared such a list of specific tasks to be performed, in what we believe to be a logical form, and I will be happy to submit it to you for your consideration and action if this would be helpful.

The need for a survivable, high data-rate, flexible, user-to-user communications is of overriding importance. We do not know of any comparable alternative system proposals to attain this capability and we believe that the Air Force should move swiftly to implement the research and development program proposed herein.

The orderly development program outlined offers the promise of a marked increase in communication capability with minimum risk. If the military situation makes it necessary, the research and development program could be accelerated. For highest payoff per dollar risked it should be remembered that communication system development is normally a ten year lead-time cycle process. Much better work in this field appears to result from a small number of people working on a project for a long period of time than from a large massive crash effort attempting to generate a complete system within a short time. It is hoped that the guidance of the suggested technical advisory panel will provide for flexibility and redirection of this program in the event unforeseen problems or new developments appear.

APPENDIX

ON DISTRIBUTED COMMUNICATIONS:

List of Publications in the Series

- I. Introduction to Distributed Communications Networks, Paul Baran, RM-3420-PR.

Introduces the system concept and outlines the requirements for and design considerations of the distributed digital data communications network. Considers especially the use of redundancy as a means of withstanding heavy enemy attacks. A general understanding of the proposal may be obtained by reading this volume and Vol. XI.

- II. Digital Simulation of Hot-Potato Routing in a Broadband Distributed Communications Network, Sharla P. Boehm and Paul Baran, RM-3103-PR.

adaptive Routing.

Describes a computer simulation of the message routing scheme proposed. The basic routing doctrine permitted a network to suffer a large number of breaks, then reconstitute itself by rapidly relearning to make best use of the surviving links.

- III. Determination of Path-Lengths in a Distributed Network, J. W. Smith, RM-3578-PR.

Continues model simulation reported in Vol. II. The program was rewritten in a more powerful computer language allowing examination of larger networks. Modification of the routing doctrine by intermittently reducing the input data rate of local traffic reduced to a low level the number of message blocks taking excessively long paths. The level was so low that a deterministic equation was required in lieu of Monte Carlo to examine the now rare event of a long message block path. The results of both the simulation and the equation agreed in the area of overlapping validity.

IV. Priority, Precedence, and Overload, Paul Baran, RM-3638-PR

The creation of dynamic or flexible priority and precedence structures within a communication system handling a mixture of traffic with different data rate, urgency, and importance levels is discussed. The goal chosen is optimum utilization of the communications resource within a seriously degraded and overloaded network.

V. History, Alternative Approaches, and Comparisons, Paul Baran, RM-3097-PR.

A background paper acknowledging the efforts of people in many fields working toward the development of large communications systems where system reliability and survivability are mandatory. A consideration of terminology is designed to acquaint the reader with the diverse, sometimes conflicting, definitions used. The evolution of the distributed network is traced, and a number of earlier hardware proposals are outlined.

VI. Mini-Cost Microwave, Paul Baran, RM-3762-PR.

The technical feasibility of constructing an extremely low-cost, all-digital, X- or K_u-band microwave relay system, operating at a multi-megabit per second data rate, is examined. The use of newly developed varactor multipliers permits the design of a miniature, all-solid-state microwave repeater powered by a thermo-electric converter burning L-P fuel.

VII. Tentative Engineering Specifications and Preliminary Design for a High-Data-Rate Distributed Network Switching Node, Paul Baran, RM-3763-PR.

hot potato

High-speed, or "hot-potato," store-and-forward message block relaying forms the heart of the proposed information transmission system. The Switching Nodes are the units in which the complex processing takes place. The node is described in sufficient engineering detail to estimate the components required. Timing calculations, together with a projected implementation scheme, provide a strong foundation for the belief that the construction and use of the node is practical.

VIII. The Multiplexing Station, Paul Baran, RM-3764-PR.

A description of the Multiplexing Stations which connect subscribers to the Switching Nodes. The presentation is in engineering detail, demonstrating how the network will simultaneously process traffic from up to 1024 separate users sending a mixture of start-stop teletypewriter, digital voice, and other synchronous signals at various rates.

IX. Security, Secrecy, and Tamper-Free Considerations, Paul Baran, RM-3765-PR.

Considers the security aspects of a system of the type proposed, in which secrecy is of paramount importance. Describes the safeguards to be built into the network, and evaluates the premise that the existence of "spies" within the supposedly secure system must be anticipated. Security provisions are based on the belief that protection is best obtained by raising the "price" of espied information to a level which becomes excessive. The treatment of the subject is itself unclassified.

X. Cost Estimate, Paul Baran, RM-3766-PR.

A detailed cost estimate for the entire proposed system, based on an arbitrary network configuration of 400 Switching Nodes, servicing 100,000 simultaneous users via 200 Multiplexing Stations. Assuming a usable life of ten years, all costs, including operating costs, are estimated at about \$60 - 100,000,000 per year.

XI. Summary Overview, Paul Baran, RM-3767-PR.

Summarizes the system proposal, highlighting the more important features. Considers the particular advantages of the distributed network, and comments on disadvantages. An outline is given of the manner in which future research aimed at an actual implementation of the network might be conducted. Together with the introductory volume, it provides a general description of the entire system concept.

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON, D.C.

11 OCT 1965



Mr F. R. Collbohm
The RAND Corporation
1700 Main Street
Santa Monica, California 90406

Dear Mr Collbohm:

The RAND Recommendation to the Air Staff - Development of the Distributed Adaptive Message-Block Network has been reviewed by the Air Staff. Major James Singleton of my Command and Control Group (AFRDQPC) has been designated as Project Monitor.

Plans are to direct AFSC to prepare a Preliminary Technical Development Plan (PTDP). This PTDP will be referred to the DCA for review to solicit their support for subsequent submission to DDR&E. (S)

We will continue to inform you of progress on this project.

Sincerely,

Glenn A. Kent

For and in the absence of:

JACK J. CATTON

Major General, USAF

Director of Operational Requirements &

Development Plans, DCS/R&D

1965

Attachment #5

Attachment #5

S	M	T	W	T	F	S
JANUARY 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
FEBRUARY 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					
S	M	T	W	T	F	S
MARCH 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
APRIL 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
MAY 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
JUNE 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
JULY 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
AUGUST 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
SEPTEMBER 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
OCTOBER 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
NOVEMBER 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
DECEMBER 1966						
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				
S	M	T	W	T	F	S
JANUARY 1967						
1	2	3	4	5	6	7
8	9	10	11	12	13	14

[illegible]

WEDNESDAY

FEBRUARY 1968						
S	M	T	W	T	F	
				1	2	
4	5	6	7	8	9	
11	12	13	14	15	16	

1

5+ hours

SUNDAY

MONDAY

TUESDAY

October
1967

1

2

3

Visitors -
N. Carr
N. 10:30 - 11:00 AM
Lunch - 11:30 (HR)
at Penn. State
Lunch - 11:30 (HR)

8

9

10

3:15 Mike Alpert
UCLA

15 Ch. to D. Lohel ✓

16 Goss Spindle?

17

22

23

24

NCC
Chicago

29

30

9:30 to 2 PM
31 TKPA
Shapiro
Klein
Shapiro
AT PA Wilson

NOVEMBER 1967

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

DECEMBER 1967

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

JANUARY 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

FEBRUARY 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

MARCH 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

APRIL 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

MAY 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

JUNE 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

JULY 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

AUGUST 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

SEPTEMBER 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

OCTOBER 1968

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

November 1967

SUNDAY

MONDAY

TUESDAY

DECEMBER 1967

S	M	T	W	T	F	S
						1
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

JANUARY 1968

S	M	T	W	T	F	S
						1
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

FEBRUARY 1968

S	M	T	W	T	F	S
						1
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29		

MARCH 1968

S	M	T	W	T	F	S
						1
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

APRIL 1968

S	M	T	W	T	F	S
						1
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

MAY 1968

S	M	T	W	T	F	S
						1
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

JUNE 1968

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

JULY 1968

S	M	T	W	T	F	S
						1
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

AUGUST 1968

S	M	T	W	T	F	S
						1
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

SEPTEMBER 1968

S	M	T	W	T	F	S
						1
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

OCTOBER 1968

S	M	T	W	T	F	S
						1
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

NOVEMBER 1968

S	M	T	W	T	F	S
						1
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

5

6

7

Election Day

09:30 Dr. Teitelbaum
Charles Dinkins in
town
12:00 Adelson SDC

12

Ch. to D. Lebel

13

9AM - Swedish Vester
9AM -
Larry Roberts
to alt lunch
Ant. Swickin
~ Here ~ 2:15 PM
Larry Roberts
IMP Committee

14

19

John F. Thirle?

20

21

Test Menial
11:30 AM
Business Week

← Alice out

26

See Guro

Tygonia - Seattle

27

ACM Guest Lecture

Seattle

28

Pullman
W. L. Spier

WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
1 2 PM - George Spauld	2 12:00 Dadikins Rus. H. Melstaf Douglas ~ 9:30+	3 1:30 - Lonsday 1/2 G.I.A. 3:45 3:45 Shalegint on this weekend →	4
8 Evening - NM Barry White	9 RAND B. F. T. Keith Gibbons Don Pernie 3 PM - State Dept of Health	10 Rana Talk in Las Vegas Gov. Commission on Comm. - 8 PM - Norman Warner	11 Veterans Day H. Minion Rover PM W. Ware BPA
15 FCC Gribble session	16 Fort Myers H. S. 6:30 Anaheim - 7 PM - Kleinrock UCLA - IMP Nelly	17 3:30 a.m. Holmes Ticket to San Juan You when we return	18
22 10 AM - G. P. Penn MCR	23 Thanksgiving	24	25
29 Stanford	30 sent ch to D. L. L.		

Memoranda

Packet Switching

Paul Baran

1. Introduction

What is packet switching? The *Data Communications Glossary*⁽¹⁾ defines packet switching as

... a data transmission technique whereby user information is segmented and routed in discrete data envelopes called packets, each with its own appended control information for routing, sequencing and error checking; allows a communications channel to be shared by many users, each using the circuit only for the time required to transmit a single packet; describing a network that operates in this manner.

Tobagi et al. ⁽²⁾ provide a more detailed definition:

The basic idea is to allocate some of all of the system capacity (along some path between subscribers) to one customer at a time; but only for a very short period of time. Customers are required to divide their messages into small units (packets) to be transmitted one at a time. Each packet is accompanied by the identity of its intended recipient. In packet-switched networks each packet is passed from one packet switch to another until it arrives at one connected to that recipient, whereupon it is delivered. Packets arriving at a switch may need to be held temporarily until the transmission line that they need is free. The resulting queues require that packets be stored in the switches and it is not unusual that all packet buffers are occupied in a given switch. Thus both the switch capacity (processing and storage) and transmission capacity between switches is statistically multiplexed by subscribers. The designers of such packet networks are faced with the problem of choosing line capacities and topologies that will result in relatively high utilization without excessive congestion.

fractured

Figure 1 shows a message from subscriber A fractured into packets and sent to subscriber B. Note that each packet may use different routes.

Paul Baran • InterFax, Inc., Menlo Park, California 94025.

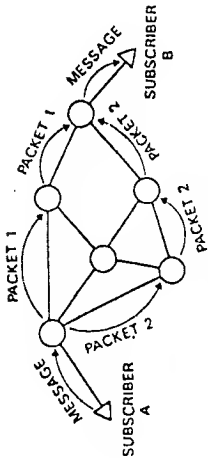


Fig. 1. Packet-switching network. (From Ross, First Edition.)

Packet switching is so flexible and powerful a set of techniques, that the system's design possibilities are entirely open. Myriad different implementations have been proposed, spawning hundreds of papers and tens of excellent books on the subject. Most of this literature focuses upon low-data-rate systems, for example interactive time-sharing computers. Yet, the underlying principles remain valid for all systems, including the new very high speed applications now emerging, including full motion video. In this context, this chapter views the communication switching challenge for the future to be the design of a "network of networks" of different types, topographies, configurations, and characteristics that must all be interconnected one day. Here is where packet-switching techniques prove to be of unique value—as the glue that can tie different parts of different systems together to allow them to operate as a coherent entity.

In this chapter the rationale for the building blocks of packet switching is described, followed by a description of three representative modern packet systems. The chapter concludes by examining the reasons that communication systems of the future are expected to become composite systems, comprising elements of both circuit switching and packet switching, working together as an integrated whole.

2. History

Let us retrace some early steps to see why and how this direction of system architecture came about—why packet switching had to be invented. In brief, it was in response to requirements that could not be readily met with the then known alternative approaches.

2.1. The Initial Requirement

Packet switching stemmed from a national defense need—how to build very robust communication networks able to withstand destruction of many nodes by an enemy yet allow the physically surviving nodes to intercommunicate among themselves. The earliest work was done at the RAND Corporation.⁽³⁾

A distributed network (one without a hierarchical structure) was found to be very robust, provided each node was redundantly connected to its neighboring nodes. In Fig. 2 we see three different types of networks. The first (A) is

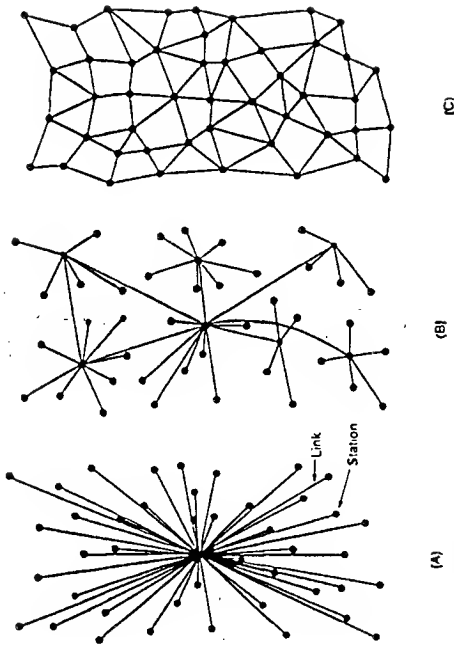


Fig. 2. Centralized (A), decentralized (B), and distributed (C) networks. (From reference 2. Courtesy of the Rand Corporation.)

called a *centralized network* because all nodes are connected to a central switching point. Communication from any node to any other node is via this central switching node. This arrangement allows simple switching. But the network has a single point of high vulnerability.

The *decentralized network* (B) is more common. Instead of a single common node, the network comprises small centralized clusters. Most traffic tends to go to the nearby neighbors. Only the longer-distance traffic is sent on the longer links. This decentralized topology is the most common configuration.

The *distributed network* (C) is the most robust of all. There is no single node point of vulnerability that can bring down much of the network. However, switching traffic around such a network is more complex than with the other networks. The complexity of switching in such a network led to the development of packet switching. How much redundancy of connection do we need?

In Fig. 3, the results of a study of the survivability of a large (20 nodes by 20 nodes) distributed network is examined. A Monte Carlo modeling approach was used. A preassigned probability of destruction was assumed for each node. The computer assigned each node a random number from zero to one. If the probability of a node being destroyed was assigned a value of 0.2, and if the random number for that particular node was 0.2 or less, then that node was assumed to be destroyed. This test was performed on each node in the network. We sought to determine the size of the largest group of nodes that could talk to one another after destruction, assuming that we had perfectly intelligent switching, in other words, if a path existed, it could be found. The results of many test runs are plotted as a curve in Fig. 3. We repeated this exercise, changing the number of individual links attached to each node. We define this as *redundancy* (of connection). For example, a network with the absolute minimum number of links needed just to connect each node together in a very

2.2. The Routing Problem

The kicker was that in those days (around 1960) we did not know how to build communication switches where messages could traverse many serially connected nodes and still operate reliably in the face of damage. We needed a new way to get a message through a large number of nodes, via circuitous paths that could not be determined in advance. And it had to pass the messages along without errors. It was obvious that the data format would have to be in digital form to avoid analog link distortion buildup, and that the routing information would have to be combined with the data itself—in-band signaling.

2.3. Flooding

The earliest networks of this survivable type proposed a "flooding" algorithm. Each node that received a message would relay it out on all connected links. The message would then circulate throughout the network. Of course, the message could rattle around forever unless some rule was applied that turned off the transmission after the message was received. One way of doing this was to keep a copy of recent transmissions. If the incoming message matched a previously received message, then it is safe to ignore this incoming message. It is clear that the incoming message had already been received and relayed. While such primitive types of "flooding" approaches work, the whole capacity of the network is tied up in sending a single message, not a very efficient way to proceed.

2.4. Back to the Drawing Board

Efficiency was not initially viewed as an issue, as inefficient flooding routing approach was first proposed for a solution to what the military euphemistically called the "minimum essential communication problem." If the term "minimum essential" is believed, you do not need a high data rate. However, "minimum essential," upon further examination, turned out to be one of those wonderfully meaningful phrases that by its nature is undefinable. History finds in periods of extreme stress everyone feels it necessary to communicate with everyone else. One lesson learned was that, like money, whatever amount of communication capability is offered, it will never be regarded as wholly adequate. Someone always wants more.

The challenge became one of creating a generalized communication switching structure. It had to be able to dynamically route high-bit-rate traffic among a large set of potential users, where each user's requirement could not be predicted in advance.

2.5. Digital Transmission Coming

At the time that this work was being conducted, digital communications was in its infancy. Bell Laboratories was publishing papers on their excellent

* For example, the total overload of the telephone system after the Kennedy assassination.

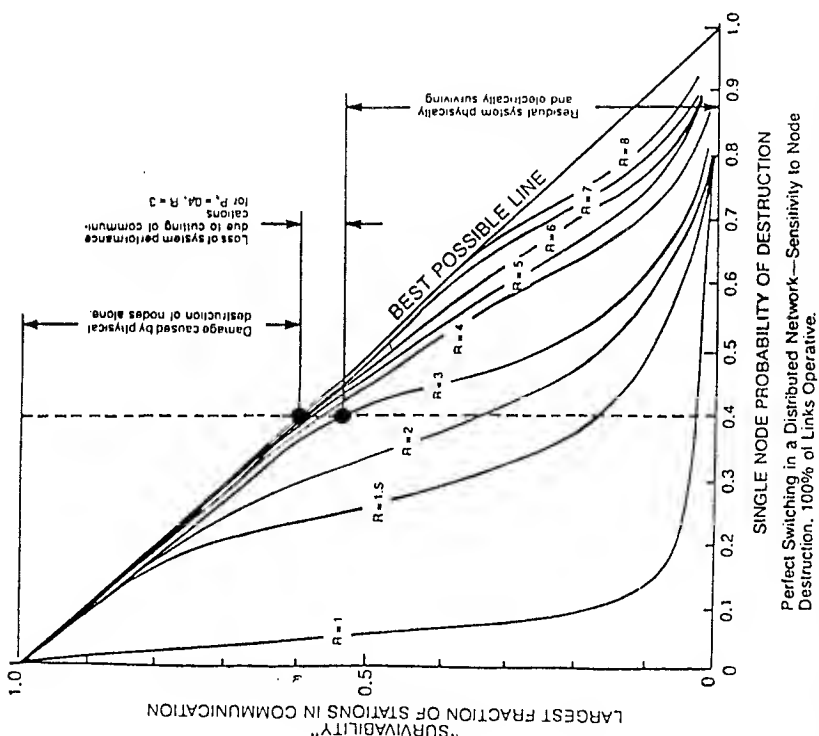


Fig. 3. Survivability of a distributed network. (From reference 2. Courtesy of the Rand Corporation.)

large network (as a long string) is said to have a redundancy level of one, or $R = 1$. If each node was connected with twice that number of links (say by having all the horizontal nodes connected together and all the vertical nodes together in fishnet fashion), then we define this as redundancy level $R = 2$, and so forth. We can see in Fig. 3 that when we reach redundancy levels on the order of $R = 3$ or 4, the network becomes very "tough." If a node survived the physical damage, then there would be an excellent chance of this node being able to be physically connected to all other surviving nodes, in the largest single group of surviving nodes. This in turn meant that it would be theoretically possible to build extremely reliable communication networks out of low-cost unreliable links, provided that we used about three times the number of links as the minimum number of links required to connect the nodes of the network together. In other words, if the redundantly connected node survived the attack, and if somehow it was possible to find and use a path through the network, there would be a high probability of being able to reach the other surviving nodes. "Somehow" is the issue.

work describing how a chain of regenerative amplifiers could be used in lieu of loading coils on existing twisted-pair cables to carry 1.54 Mbps. (This is now the T-1 or DS-1 rate transmission technology.) This high speed all-digital channel would clearly be the ideal building block for all future digital networks. And it meant that we should start thinking of switching megabits per second data rates—commensurate with the data flow rates within digital computers. This in turn opened the option to begin to think in terms of switching nodes built wholly around digital computer technology, with switching in memory rather than using cross points, and with the nodes connected together using high-data-rate links.

2.6. Synchronization

The data flow in the network had to traverse many tandem nodes. It is extremely difficult to have all individual links in tandem operate at the exact same data rate as required for a circuit switch connection. Why not then operate each link at its own "natural" data rate? Each switching node, being a computer, could provide the buffering to remove the need for tight overall network synchronization timing. This simple choice meant that we could now totally avoid any physical real-time connection between the transmitting and receiving end user. Yet, if the data rate was fast enough, the user could be left with an illusion that a real-time connection existed.

Parenthetically, all this may seem to be obvious and trivial today. But at that time this now obvious point encountered a mental brick wall in the minds of many competent communication engineers. There was a conceptual barrier in comprehending the scheme, particularly for those not well versed in the digital computer art.

2.7. Adaptive Routing

The necessity of finding paths through a network of changing topology because of random damage meant that we needed a way to route data through the network on an adaptive learning basis. The analogy that we chose was a letter and an observant postman at each node (or post office).

Each "postman" at each node derives the best route to every station in the network by observing the return address (the "from" field of a packet) together with a number corresponding to the letter's cancellation date. We called this date stamp the *handover number*. Every time the letter (packet) was relayed from node to node, the handover number was incremented by 1. Thus, our hypothetical local postman, by observing traffic passing through the node and by recording the handover numbers of the FROM station together with the link number over which it came, determined the best outgoing link.

In Fig. 4a we view that hypothetical mail system, composed of routes (links) between post offices (nodes). We assume that no post office has knowledge of the location of any other post office, other than what can be

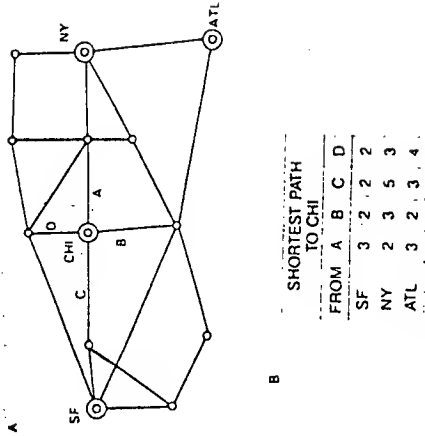


Fig. 4. Adaptive routing—the hypothetical postman.

inferred by looking at the cancellation dates of the mail passing through the local post office.

The postman at each post office records the most recent cancellation dates observed for each origination post office, as shown in Fig. 4b. Each postman observes the same rule. The rule is to send out each outgoing letter via the route (link) that showed the latest cancellation date of mail received from that address. When the system starts up, there is a bit of chaos as the letters randomly go from post office to post office. But this stabilizes quickly.

In Fig. 4b we see that the Chicago postmaster has learned that if he sent a letter to New York and took outgoing route C, it would not likely take less than four hops, whereas if he sent it out on route A it would be two hops or more. Since 2 is better than 4, the postmaster would choose to send the New York-bound letter out on route A. But if route A was unusable, routes B or C would be good alternatives.

With each node in the network following the same set of rules (algorithms), simulation showed that the network was soon routing traffic very efficiently. This means that if a node had an indication of the duration of a message in the network, it has information needed to route future traffic in a fully distributed network, without centralized knowledge. The same scheme is easily modified to "forget" as well as learn so as to be able to adapt to failures in the network.

Each letter is always sent out on the instantly available best route toward its end destination. If the best route was busy or dead, then the second best was chosen, and so forth. Each node was even allowed to send the packet back if no other better route were available. Each packet was described as a hot potato for which the postman did not wear gloves, to suggest the speed of the relay sought. Thus, this early routing scheme is called the *hot potato routing algorithm*.

2.8. Where the Name Packet Came From

In those days (around 1964) we used the term *message block*. Two years later Donald W. Davies, of the National Physical Laboratory, unaware of this earlier work, independently came up with a related approach. Davies used the term *packet*, a far better and a more graceful term of British usage, from which we get our present day term, *packet switching*.⁽⁴⁾

3. Characteristics of the Packet

3.1. Packet Length

The initial system description in the RAND papers was in terms of a 1024-bit packet. This number was chosen as a compromise. If the packet length is much shorter, there is a loss of data rate because of the fixed overhead information in the header. Alternatively, as the packet length increases so does the probability of a single bit error, which would require the retransmission of the entire packet and a resulting loss of efficiency. Today, the number of bits per packet is usually about 100 to 10,000 bits. The optimal packet length as a function of throughput tends to be a flat-bottomed U-shaped function.

3.2. Fields

You need a way to delineate the start point of a packet. This is now called the *flag*. Detection of the predefined flag alerts the node that a packet is arriving. The identification of the flag starts the process of separating out individual parts of the packet. Similar to an envelope going through the post office, you need a "to" address and a "from" address. The bit space reserved for each part of the packet is called a *field*. The size of each field is a function of the size of the network. For example, if you expected up to 64,000 users on the network, a minimum of 16 bits would be needed for the "to" address and another 16 bits for the "from" address ($2^{16} = 65,536$).

3.3. Error Detection

One housekeeping field almost always used in low-speed packet switching is dedicated to *error detection*. Think of it as a check sum. The original RAND plan proposed a cyclical redundancy check (CRC) sum, still the preferred error detector today. The CRC approach provides a powerful and efficient error detection test. If the error detection test fails, no acknowledgement is sent and the packet is retransmitted. A selected binary prime number polynomial is used at the transmitting and receiving ends of each link, with the entire packet being regarded as a single long binary number. This binary number, which uniquely represents the packet, is divided by the CRC polynomial. This is a binary long-division operation. The remainder of the operation is inserted into the

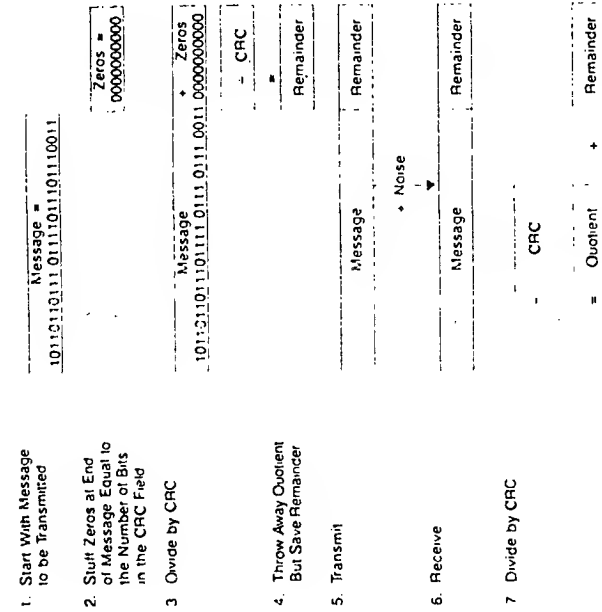


Fig. 5. Error correcting code—CRC.

CRC field. The quotient and the remainder are transmitted. Upon receipt, the inverse of the process is performed. If no error occurred, then the result of the inverse multiplication of the quotient produces a remainder with all zeros. If the remainder is not all zeros, we assume that the packet has not been correctly received. While it is always possible to use error-correcting codes, it is easier to detect that an error has occurred and by nonacknowledgment request a retransmission of the defective packet.

Figure 5 shows the process by which a CRC is added to a message to be transmitted together with the process for using the CRC to ensure that no errors have occurred. It may look complicated, but it is really an easy algorithm to implement. It is powerful, in that it is not sensitive to errors occurring in a block, which defeats simpler schemes to catch errors. Any single bit error drastically changes the whole message. This eliminates the possibility of two separate errors from creating the illusion of no errors.

3.4. Acknowledgment

To ensure no known loss of packets in applications where absolute data integrity is required, an acknowledgment is granted for each correctly received packet. Generally an acknowledgment of the properly received packet is required before the responsibility for further relaying action is transferred.

nonacknowledgment is usually called an ACK message. And a negative or nonacknowledgment is sometimes called a NAK.

In the original hot potato routing algorithm, a lack of a prompt acknowledgment meant that the same packet would be sent out over another link rather than waiting and retrying the original link. Such system choices vary from system to system. There are lots of alternative design choices that can be made in packet systems.

3.5. Order of Arrival

Allowing sequential packets to travel by different paths means that some packets will take longer paths than others. This means that some of the packets could arrive out of order. To deal with this possible problem, a field in the header is dedicated to carry a short serial number to indicate the sequence of packets sent. The receiving unit notes the short modulo serial number to sort the received packets into their correct sequence buffers. When the buffers are read out serially, each packet would then be in its correct order. The number of buffers required in practice is a function of the data rate, and the expected variance of the delays of the transmission paths.

Figure 6 shows the scheme used to catch and remove errors caused by the packets taking different paths and arriving out of order. In Fig. 6a a series of packets is being sent from a transmitting station on the left and received on the right. The first two packets, 1 and 2, have arrived in their proper order. As can

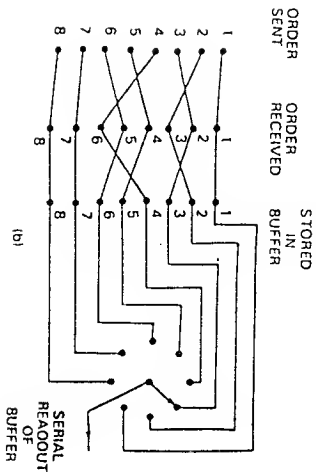
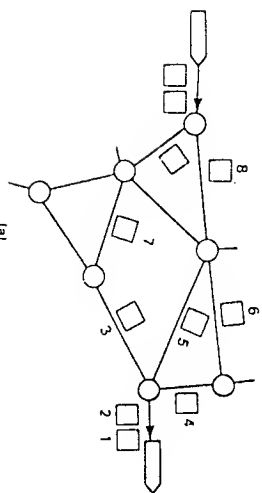


Fig. 6. Modulo 8 sorting to prevent packets from being received out of order.

be seen, the packets could take different paths and arrive out of order. To unscramble these crossed-over packets, we use the approach shown in Fig. 6b. The first column represents the order of the original packets. The next column represents the packets in actual order received. The third column represents a series of eight buffers. The packet with serial number 1 is to be put into the first buffer. The packet with serial number 2 is placed into the second buffer, etc. The drawing shows a hypothetical rotary switch to dump the contents of each buffer sequentially to allow the packets to exit in their original order—first in, first out.

4. User Interface to the Network

To this point we have considered only the switching nodes part of the network. Let us now move on to consider the means of connecting users into the packet-switched network. We would like to have many different users connected to each switching node and be able to address each user separately. In the RAND proposal, the term *multiplexing station* was used as the interface between the user and the switching node, wherein each user had a unique address.⁽³⁾

Figure 7 shows the concept of the multiplexing station. The circles represent the switching nodes, described earlier. What is now introduced is a packet-based statistical multiplexing station that allows many simultaneous

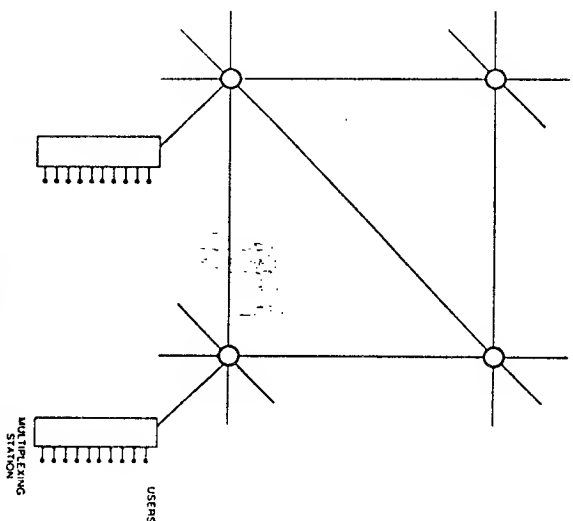


Fig. 7. The multiplexing station.

lower-data-rate users to share a common high-speed channel. The traffic from a number of users at one location is sequentially multiplexed packet by packet. Each user's packets are sent as independent freight cars in a long freight train. Each freight car is destined for a different location, but set off on their journey together. Of course, each user must now have its own local mailbox address, rather than only the address of the switching node as in the previous discussion. On the receiving end each multiplexing station uses terminating buffers dedicated temporarily to each end addressee.

4.1. Statistical Multiplexing

silence = unused memory

In most communication applications, silence is the *usual message*. In other words, no true information bits are transmitted most of the time (i.e., remote computer terminals, voice, two-way video, etc.). There is an economy to be gained by not sending long strings of 0's or 1's that contain no information, as is done in circuit-switched networks. The magnitude of this economy can be large. We are thus able to build packet networks where the total throughput capacity can be far less than needed to handle a theoretical peak traffic, if we had assumed that all users actively have sent data at the exact same instant, which they never do. Thus, an implicit ground rule of packet switching is to avoid sending a packet unless it represents true information. If there is no change in the data stream relative to the contents of the last packet, why bother sending a packet? It adds nothing.

Most time spent on interactive timeshared terminals, for example, is thinking time. The average transmitted net data rate is low. Thus, there is significant economic advantage in the multiplexing function inherent in packet-switching data networks. In effect, we multiplex resources across the whole network rather than just on a single line at time. The larger the pool of users multiplexed together, the more effective is the process.

4.2. Creating Virtual Circuits

The packet network has the responsibility to provide the connected user with the missing nontransmitted packets to maintain an illusion for the user that his or her computer is always connected. This concept is called a *virtual circuit*. There is no limitation to the number of virtual circuits that can be simultaneously maintained, provided that each is terminated into a process that fakes out the connection. *The virtual circuit concept underlies the attractive economics of packet switching.* You create an illusion of a circuit that is always there when you want it. But it consumes no resources when not instantly needed. It is the fast speed of the switching that allows the sleight-of-hand to create the illusion of a physical connection.

In Fig. 8 we revisit Fig. 7 and remap the drawing from the point of view of the multiplexing stations. We show the remainder of the network as a fuzzy cloud to emphasize that the user does not particularly care how his traffic gets to its destination. The user need not be concerned about the transportation portion

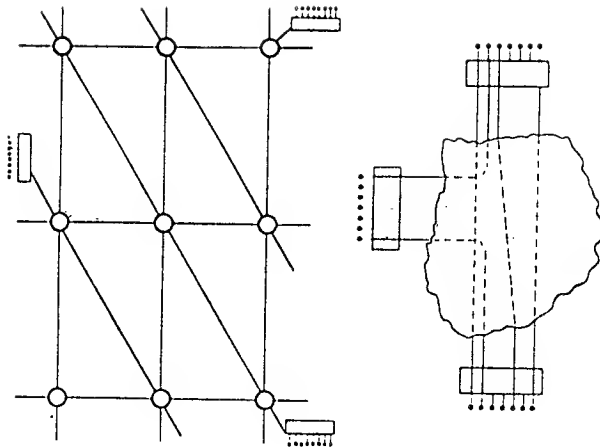


Fig. 8. Virtual circuit concept.

of the network. Rather, all the user sees is a *virtual circuit* to the chosen end destination. The user cannot tell the difference between a physical and a virtual circuit by virtue of the asynchronous time division multiplexing of the packets.

4.3. System Overload

Every system has a maximum allowable load. Network performance is limited by the number of packets that can be sent per unit time without overloading any network component. It is important that the packet network be designed to overload gracefully. The situation is like a network of roads. If there is too much traffic, the average speed of all the automobiles on the road will decline. Add more traffic when things are getting worse, and you bog down the whole system. Similarly, with packet networks, you must be careful not to overload the network. You cannot stuff more packets onto the network than it can digest without getting indigestion. This preventative process is called *flow control* or *congestion control*. For example, in the case of freeways passing through urban areas where heavy new traffic can enter from side streets, traffic lights are sometimes used to block the new flow of automobiles. On Interstate 280 in Santa Clara, California, for example, during rush hours some traffic lights allow only one car at a time to enter the freeway from the side streets. The rate of acceptance of new cars is varied as a function of the freeway's traffic speed, or the road's ability to get rid of the through traffic. This is flow control. Flow control is an important concept in the design of packet-switching networks. The

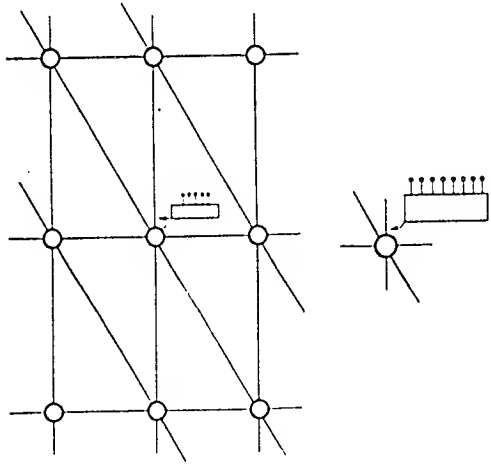


Fig. 9. Congestion (load) control

subject of how best to maximize flows (and/or minimize delays) has merited many papers examining different approaches to the routing and control process to maximize total flows. Several interrelated parameters must be kept in mind. Sometimes parameters other than total flow are optimized, such as transit times or guaranteed maximum packet time delay. Some approaches seek to achieve maximum "fairness" where priority may be given to lower-data-rate users relative to big "hog" users to best share the common resource.

In Fig. 9 we see a network comprising switching nodes, shown as circles, plus links connecting them together. The arrows represent a heavy flow of traffic from the lower left to the upper right. In this network is a multiplexing station that we assume to be generating an additional traffic load into the network. As the traffic density increases, the longer-path background traffic would tend to flow away from this busy node, taking other paths and thus increasing path lengths. But suppose many multiplexing stations all did the same thing at the same time? Then network overload would occur and could bring down the network. To prevent this potential disaster, means for preventing the addition of new traffic into the network are needed. The flow control's purpose is to throttle back new loads to prevent overload by giving priority to traffic already flowing in the network. In practice, a good packet-switching network is a compromise between load-carrying ability and delay time.

4.4. Importance of Analyses

The great flexibility open to the designer of a packet switch means that the designer must consider complex models and optimize several interactive parameters. As we have seen, unconstrained loads can cause the networks to

fail. The well-designed network avoids danger points in which the network could become unstable and break down, similar to automobile traffic gridlock. Such undesired behavior is avoided by careful design of the network. This topic is beyond the scope of this book. Chapter 3 provides a discussion of the basic elements.

4.5. Reason for Reliability and Low Error Rates

Why is packet switching so reliable a data transmission scheme? There are two reasons: the redundancy of the routes allowed, and the policy of keeping a "carbon copy" of the transmitted packet until you are "absolutely positive" that the packet sent has been correctly received by the next recipient. If in doubt, you "fail-safe" and retransmit the packet. You let the end point clean up the duplicates. The "absolutely positive" assumption derives from the use of redundant information in the packet—the error detection field (i.e., the checksum or CRC data). This ensures that the data have never been corrupted in the transmission process. The slight message redundancy contained in the CRC performs the same function as the redundant coding of the DNA molecule. The DNA molecule must be duplicated through many generations of copies. A slight inbuilt coding redundancy in structure prevents incorrect copy of the molecule from ever being made, except in very rare instances. With packets, the original copy is always retained until there is certainty that the packet has been perfectly copied. Replication thus occurs generation after generation without error. There is always a residual low probability of error, but its value can be made arbitrarily small by a longer CRC or end-to-end verification.

4.6. Encapsulation

Another key property of the packet derives from its intentional design as a wholly self-contained letter. Any letter can be encased within a sealed envelope, which can in turn be encased in another envelope as shown in Fig. 10. The outside of each envelope contains all the necessary addressing information at the concatenated level of interest. At each level, the envelope (header) can be stripped off and discarded after use. Only the header is needed for routing. Thus, for example, the internal contents can be encrypted for privacy while the outside envelope—the header—is not, to allow for its delivery. This packaging allows a total division of responsibility at the packet interface. The freedom to insert one letter-including envelope into another envelope can be concatenated as often as desired. *This is the key for interconnection of different subsystems.* This process, called *encapsulation*, is the reason why packets can be so easily transmitted through totally different types of packet networks, each with its own peculiar protocols. For example, imagine two different networks, each with its own set of rules of operation, and where user A on network A wants to send a data stream to user B in network B. See Fig. 11.

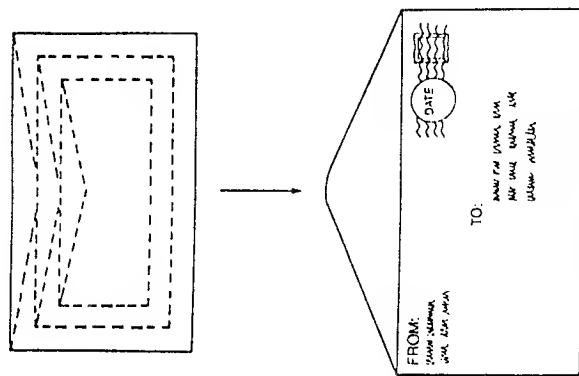


Fig. 10. Encapsulation.

Further assume that networks A and B are old packet networks built in an earlier era when there was no requirement to send traffic between A and B. The managers of networks A and B have gotten together. They have now decided that they want to allow users in either of their two networks to be able to intercommunicate. But, they do not want to change any of the internal

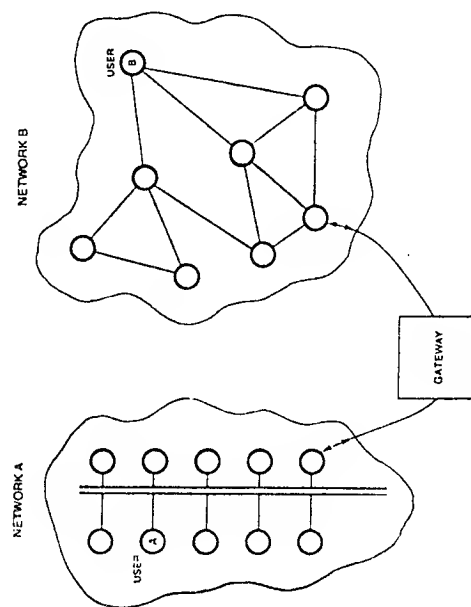


Fig. 11. Use of a gateway to communicate across system boundaries.

operations within either network. They want to spare the cost and inconvenience of the change to existing customers on each network, who have no need to communicate on an internetwork basis. A "gateway" is created between the two networks. Traffic destined to users on the second system uses a two-envelope or encapsulated packet approach. The first envelope is addressed to the gateway for transmission across the gateway link. The received packets are stripped of their envelopes (decapsulated) and sent on to their final destinations following all the procedures of network B.

The ability to readily be able to insert one packet within another and within another recursively in a concatenated manner is the key tool to allow interconnection of totally different types of networks. This technique allows data to be moved from layer to layer of the open systems architecture hierarchy of protocols (which we discuss later) to interconnect different types of systems. What is so magical about packets? Could we not do the same thing with a circuit-switched connection? Yes. But, in the real world when it is necessary to change data rates, character definitions, signaling formats, etc., it is a much simpler design task to simply use packets. You do not have to change the entire system, just one level of the concatenated system units.

4.7. Asynchronous Nature

Packets are best viewed as wholly contained information entities designed to match the characteristics of the network switches. In a computer-based packet switch, the computer ideally has overall control of timing and not the transmission link. We only have to tell the software-driven computer, "please complete each task within an allowable time period." And by allowing a little slop in the time dimension, we totally remove the constraint of absolute bit-by-bit timing. We need this "rubber" in the timing for the communication system to ask for and receive retransmission of defective packets. This in turn allows the designer to use data buffers and to make best use of the potential computational capacity of the switch. It means that a large number of totally different formats can be handled, and each can be differently defined in software, even if each requires a different processing delay. The packet approach seeks and achieves a maximum degree of totally asynchronous performance.

Figure 12a reviews some of the characteristics of the packet we have described:

1. The routing information is shown to travel with the data in the packet.
2. Timing differences between tandemly connected links are allowed.
3. The technique of block-encoding error detection and repeat transmission is essentially error-free transmission.
4. Buffering makes efficient use of the network's capacity.
5. Protocol conversion is easy by virtue of the packet format.

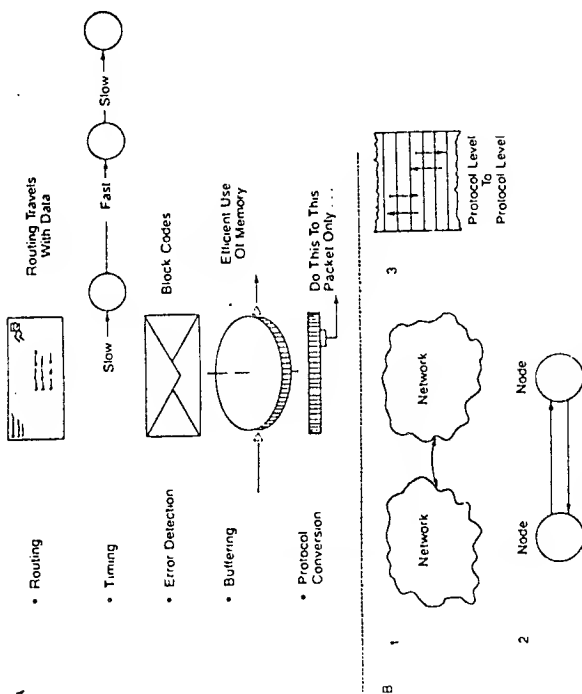


Fig. 12. Flexibility of the packet.

Figure 12b reviews how the packet creates a logical bridge (1) between different networks, (2) from one node to another node, and (3) from one protocol level to another.

5. Evolution of Packet Switching

To this point we have reviewed the basic concepts underlying the packet-switching art. In this next section we explore some evolutionary directions yielding different types of systems. Later we consider the subject of very high speed packet switching, a direction of system evolution now underway. But, now we shall go back in time and consider some of the early evolutionary directions to put the discussion that follows into context.

The initial RAND work started with low-data-rate systems—tens of bits per second (about 1960). Later, in response to demands for higher data rates (about 1962), the investigation focused on the highest data rates that could be then supported by the then computer and communication technology, 1.5 Mbps. The hypothetical platform was to be a universal national defense communication system, capable of handling all media then in use (teletypewriter, data, facsimile, and voice). Later writers characterized the early work as being solely focused on packet voice. Not really. The confusion may have stemmed from the easier access to summary versions rather than the initial papers. But it is true that packet voice was considered at the outset, it has taken 25 years before we have seen commercially viable toll-quality packet voice.

Why the delay? The reasons are many. Initially a conceptual block in understanding how these networks would work had to be overcome. You had to believe that statistics really work. If you did not, then the system cannot possibly work. The concept of a virtual circuit being there when you want to use it while others were also sharing the same resource at other times requires an almost religious trust in statistics. Many had trouble believing the simulations that indicated that a packet's travel path length will almost always (99.99%) be less than an anticipated maximum boundary limit. Those who understood statistics were inclined to believe that the scheme would work. Those who did not were skeptical.

i.e. Kleinrock

5.1. ARPANET

With the exception of Donald Davies' early work in 1966,⁽⁴⁾ the first real packet-switching system ever built was the ARPANET by Lawrence Roberts.⁽⁵⁾ The ARPANET was, in part, an experimental verification of the packet-switching concept. Robert's objective was a new capability for resource sharing among the ARPANET academic research community in the information processing field. Although the packet-switching concept was first described in terms of 1.5 Mbps links, such data rate links did not exist at an acceptable price in the late 1960s. The fastest link that ARPANET used for its initial test in 1969–1970 was 50 kbps. Some links were lower speed. ARPANET served a community of low-data terminals connected to remote host computers, and host-to-host connections. The ARPANET was eminently successful in both the communication and resource-sharing applications. The economics of the ARPANET was sufficiently attractive, given the line utilization efficiency of the virtual circuit concept, that other packet-switching systems were developed shortly afterwards around the world.

5.2. Packet Radio and Satellite

Once the appreciation for the packet and its characteristics caught on, a number of new developments evolved. Norman Abramson of the University of Hawaii proposed packet radio (1970).⁽⁶⁾ This work was extended by Kahn⁽⁷⁾ and Fralich and Garrett.⁽⁸⁾ Abramson also proposed packet satellite in 1973.⁽⁹⁾ In the case of such half-duplex, shared broadcasts you cannot be sure that someone else is not simultaneously transmitting. Abramson shows that if the channel capacity was adequate, you could take a chance and send your packet with a reasonable probability that it would not collide with others. If it did, a retransmission is in order. This approach is named the *Aloha protocol*. Is this really a packet-switching system without a number of tandem links? Yes, if you define packet switching in the large. But it will exhibit different properties when you do not face the requirement of having to relay traffic from node to node. It looks more like a shared link rather than a full network in the usual sense.

In Fig. 13a, the Aloha system, a packet transmission system, uses radio, where each radio device cannot always hear its neighbors. Thus each radio is free to transmit its packet whenever it chooses. If no acknowledgment is

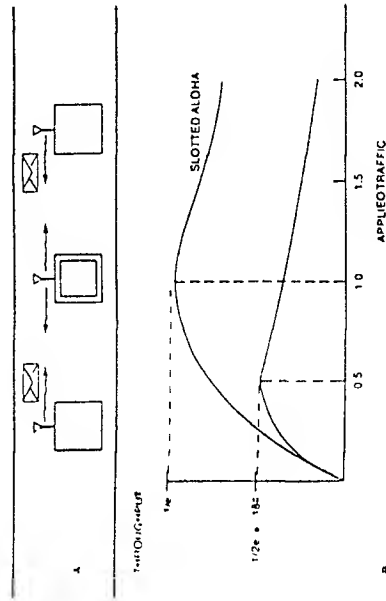


Fig. 13. The Aloha system.

received because of collision, the transmitting station would retransmit its defective packet. As the number of packets to be transmitted is increased beyond a certain rate, the increasing number of collisions will cause a decrease in capacity. See Fig. 13b. The maximum traffic rate that can be handled in an Aloha system is $1/2e$ of the maximum channel capacity, or 18.4% of the applied load. Roberts⁽¹⁰⁾ proposed time slots assigned to users in advance. This is called *slotted Aloha*. It doubles the capacity of the channel, but at some cost of complexity and freedom of access.

5.3. Ethernet

Ethernet, an early local area network, was invented by Robert Metcalfe and David Boggs at the Xerox Palo Alto Research Center (MET 76).⁽¹¹⁾ Their idea was to use a shared coaxial cable as a common transfer medium—the “*ether*.” Each node listened on the common coaxial cable. If a node on the cable wants to send a message to another node on the network, it politely listens to be sure that no one else is using the party line. Then it bursts its packet out at 10 Mbps to get in and off the line quickly so that the common channel could be shared by others. Each node on the cable listens for a carrier to determine whether anyone else is transmitting (carrier sense). The node does not transmit until the channel is clear. If the channel is busy, each node waits an increasing but independently determined random time before transmitting. This prevents two users from transmitting at the same time. Ethernet also senses collisions. This could happen, although the probability is low, given the finite propagation delay through the cable. Ethernet is thus known as a *collision detect/carrier-sense multiple-access (CD/CSMA)* system.

In Fig. 14 a coaxial line is the common shared transmission path. Electric signals are generated and received by the transceivers. Each transceiver taps into the coaxial line with a very small value coupling capacitor to avoid impairing the cable's transmission properties. The digital transceiver output is buffered and then checked for errors.

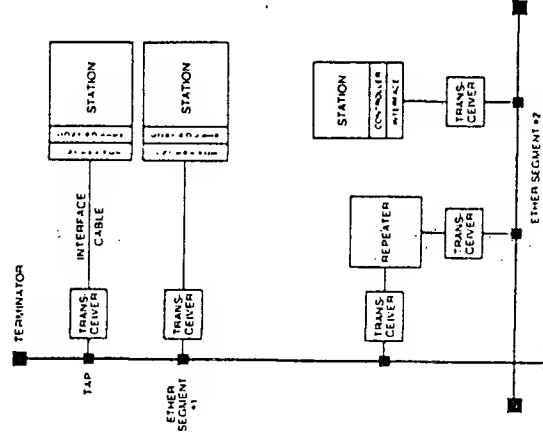


Fig. 14. Ethernet. (Reference 11.)

5.4. Varieties of Local Area Networks

Ethernet became the forerunner of the many latter-day local area networks (LANs) used to tie together computer systems and terminals, generally within a single building.

Since no single communications link or system is optimum for all applications, there was, and is, a strong tendency to devise slightly different LANs, each tailored for best fit in a single application. Sometimes cost minimization was the driving issue. Lowering the data rate and reducing the overhead in the packet allowed cheaper systems to be built. As a practical matter, the savings were short-lived because of the increased cost of separate and unique software required for each system. So many different types of LANs were created that a Tower of Babel problem of incompatibility emerged. The units could not readily talk to one another. Any savings in hardware costs were swamped out by the added costs of dealing with so many different interfaces.

6. Standards

Historically standards evolve in one of two ways. Usually, a single company's product with the major share of the market becomes the de facto standard. Alternatively, after a long procedural process between competing systems, and with political give-and-take, a compromise is reached and a consensus standard finally emerges.

In the case of packet switching, the field had barely gotten underway when the importance of interconnection became fully appreciated. The organization responsible for international communication standardization, the CCITT (Consultative Committee for International Telephone and Telegraph), is a deliberative body. It is composed of representatives of each of the interested nations. Because telephone and related communications are a monopoly in most countries of the world, the CCITT primarily represents the national postal and telephone administrations. The speed with which the many standards and protocols relating to packet switching have emerged is remarkable. Over the years a number of packet-based standards gelled to form a solid foundation of agreement, greatly simplifying the orderly development of the evolving packet-based technology.

6.1. Open Systems Architecture

The major foundation stone for the standardization activity for systems yet to be designed is the open systems architecture concept built around protocol layering.

The objective for much of this standardization effort is the creation of an open systems interconnection architecture (OSI).⁽¹²⁾ Stallings notes that the communications industry has long required that physical, electrical, and procedural characteristics of its equipment be standardized. This view differs from that prevalent in the computer industry, where in the past each computer vendor sought to monopolize its own customers. With the merging of computers and communications, customers and the communication carriers themselves are no longer willing to accept special-purpose protocol-conversion software development without full considerations for future interconnection. Agreement on standards is now mandatory because viable standards are necessary to allow products from several vendors to interoperate. This lowers costs for all by increasing the production volume for standardized units, which is preferable to short runs of unique products. There is a trade-off here since standards tend to freeze technology. But standards are at the foundation of packet system evolution, as will be seen when we return to the subject of OSI. But to put the subject into context, we review the evolution of packet switching and then suggest where the field appears to be going and why the OSI approach is so relevant and important.

7. Three Example Systems

Having talked about the general concepts of packet switching, we now consider a few sample systems to give you a better idea of how they work and to show the wide range of possibilities open to the system designer. Most packet-switching systems being built are still low-data-rate systems (operating at voice band data rates). The direction for the future is clearly toward the higher-speed versions of the technology. The three specific examples of packet

switches below are chosen to suggest the nature of the evolution of the technology, including video switching. The first example is the packet switch used as part of the common channel integrated signaling system No 7 (CCIS 7) implemented in today's circuit-switched telephone plant and important to the evolution of the Integrated Services Digital Network (ISDN).

The second application describes a commercial fast packet switch using 1.54-Mbps T-1 (DS-1 rate) links for combined voice/data applications.

The third example is an even faster packet switch, which operates with links at the DS-3 rates (44 Mbps the common fiber-optic data rate). There are even faster approaches in development, which we also briefly describe.

As we review each system example, it is helpful to observe the combination of packet switching coexisting together with circuit switching. In previous chapters we examined circuit switching, and the initial portion of this chapter focused on packet switching. The remainder of this chapter shows that the distinction between the two technologies is blurring with time. Systems designs increasingly are combining elements of packet switching together with circuit switching. It is not an either/or matter. Rather, there is a range of options along a spectrum of possibilities bounded by one extreme by pure circuit switching and, at the other end, by pure packet switching.

7.1. CCIS 7

As an example of low-data-rate packet switching, we shall use the common channel signaling No. 7 system as found in today's telephone systems. Here a conventional telephone circuit switch uses a digital packet switch subsystem for its signaling. Figure 15 shows the circuit-switching arrangement for the voice band channels, with the digital packet switch forming the common signaling channel. Analog signaling is replaced by digital messages formed into packets. This arrangement is fundamental to the evolution of the all-digital ISDN system.⁽¹³⁾

ISDN starts off with a conventional telephone-switching system. The signaling information is picked up at the first switch or *signaling point* (SP), converted and fed into a separate packet-switched signaling network node called a *signal transfer point* (STP). This packet-switched network for the signaling information ties together the STPs and is redundantly connected to all the related telephone switches. This arrangement for signaling information can be fast, if high data rates are used, and it can be robust if adequate path redundancy is used.

An increasing amount of translation takes place with dialed telephone calls. For example, if you call an 800 toll-free number, every toll switch must be able to translate this number into the desired area code and end number. To simplify matters, this information translation can be centralized. To reach the common shared data base, a packet is created and sent on the described separate packet network. One day the entire United States telephone system will be all digital, but for now voice band (600–3000 Hz) modems operating at 2400 bps can be used to exchange the packets containing signaling information while ~~1500~~

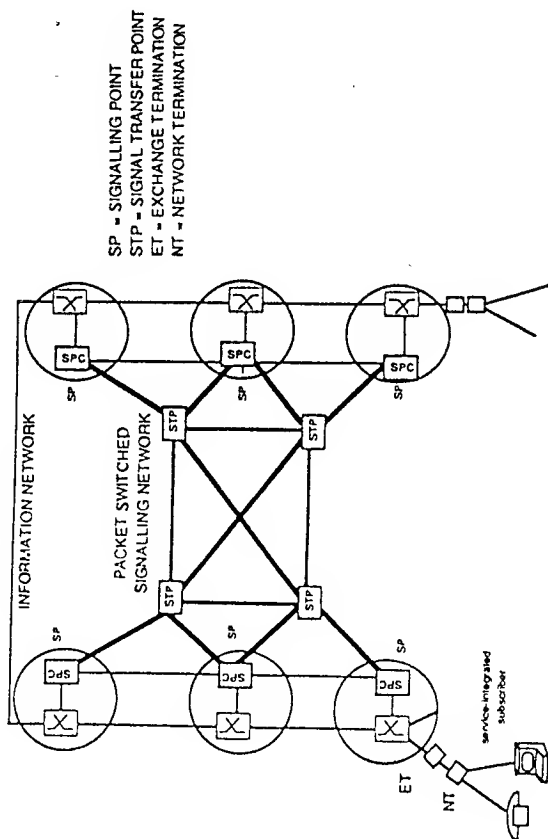


Fig. 15. ISDN information network and signaling network. (Reference 13.)

increases this rate to 64 kbps. The overall process is simple. The input telephone number is converted from the dial tone multichannel analog format into bits, and information is added about the class of the call and the origination number. Next the packet will have the usual "to" and "from" fields appended, an error detection field will be computed and appended, and the packet shipped off. Why has the use of packet switching here evolved in lieu of the dedicated control channels in the past? There are three reasons: robustness, economy, and flexibility.

Robustness derives from the characteristics of the packet switching earlier described: powerful error detection and required acknowledgment plus flexibility of routing through a redundantly connected network. The economy here comes primarily from sharing a common data base, since the care and feeding of very many separate data bases is an expensive occupation. The idea here is to put all the eggs into one basket but to take very good care of the basket. Flexibility comes from the ability to provide new services, for example, calling number display, and to look ahead to detect busy circuits on telephones.

7.2. The Economy of Packet Voice Transmission

Packet switching's early implementations were often limited to telephone voices band systems. These limited data transmission to the order of 2400 bps.

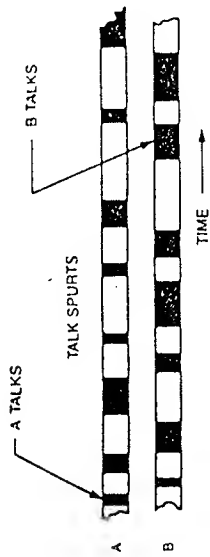


Fig. 16. Occupancy of a full-duplex voice channel.

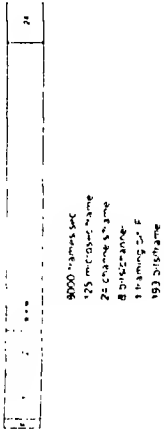
Packets were sent between terminals and to computers, and for data to/from computer to computer. The low data rates and long delay time for packets, about half a second or more, were inappropriate for voice services. As the allowable data rate on the transmission media evolved to T-1 rates, packet switching of voice became feasible. The desire to do so stems in part from improved line utilization made possible by taking advantage of blank periods of speech. For example, imagine two speakers sharing a full-duplex telephone circuit. Generally only one of the two would speak at any one time. If we suppress the spaces between talk spurts, we find that each unidirectional circuit is utilized only 40% of the time. Thus, a potential economy gain factor of about 2.5 exists. See Fig. 16.

Conventional pulse code modulation (PCM) voice operates at 64,000 bps. Adaptive differential pulse code modulation (ADPCM) provides almost as good quality voice at 32,000 bps. ADPCM is increasingly being used in transmission systems since it allows a factor-of-2 improvement in carrying capacity for digital voice.

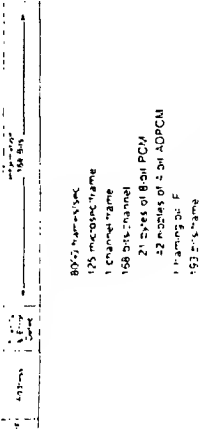
7.2.1. Economics of T-1 Transmission

Today, 1.54-Mbps T-1 digital circuits are widely available at a rental cost of only about eight times that of a single analog voice circuit. Each T-1 link normally carries 24 full-duplex 64-kbps PCM voice circuits. If packet switching with silence suppression plus ADPCM in lieu of PCM is used, a potential improvement factor of $2.5 \times 2 = 5$ occurs. Allowing for losses attributable to the packetization overhead, 96 channels of toll-quality voice on a T-1 line become possible. If the user is able to use all the purchased capacity, then each of the 96 voice channels is obtained at a monthly cost roughly equivalent to about one-twelfth that of the conventional alternative cost (not including additional costs for the packet voice and ADPCM conversion equipments). The payoff becomes even greater when data channels are intermixed with the voice channels, since most data applications do not occupy a full voice channel but generally 9600 bps or less. New, lower-data-rate voice conversion techniques are in development, which further lower the number of bits per second to support a voice circuit, thereby increasing the potential economies further. Thus the number of equivalent channels possible on a T-1 line might even be greater than the 96 channels described.

Standard O4 Frame Format:



FastPacket Frame Format:



Data Packet

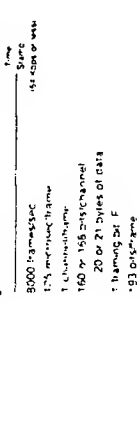


Fig. 19. StrataCom packets. (Courtesy StrataCom.)

there is contention for the channel, the StrataCom switch intentionally drops voice packets but not data packets. Loss of a single voice packet can be rendered essentially inaudible, if the last correctly received voice packet is substituted for the missing packet. Data packets have priority over voice packets and use error detection.

To minimize the delay time of voice packets and avoid its variability, once a virtual voice channel is set up, its routing path stays fixed (together with a maximum delay time) unless a failure occurs. The voice virtual circuit is the same concept as the data virtual circuit discussed in Section 5.4.2. Thus the virtual circuit formed is similar to a circuit-switched channel except that silence periods in speech are not transmitted. The dividing line between pure packet switching and circuit switching is blurred. The intrinsic packet-switching approach allows the system to retain the full advantage of fast automatic rerouting in the event of failures.

The StrataCom unit is essentially a multiple-redundant-hardware fault-tolerant software-defined computer. This software-intensive approach in lieu of casting functionality in hardware allows flexibility for user-defined system control. In essence, the real-time user is able to rapidly redefine the network's configuration remotely. Remote monitoring and changes in line assignment or characteristics, for example, can be inserted by the user via computer terminals

San Jose Group 1	Rev. 3.0	Oct 21 1987 11:22 PST	
CLN	TRR	PKT	Control Line Alarm Status
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	32
33	34	35	36
37	38	39	40
41	42	43	44
45	46	47	48
49	50	51	52
53	54	55	56
57	58	59	60
61	62	63	64
65	66	67	68
69	70	71	72
73	74	75	76
77	78	79	80
81	82	83	84
85	86	87	88
89	90	91	92
93	94	95	96
97	98	99	100
101	102	103	104
105	106	107	108
109	110	111	112
113	114	115	116
117	118	119	120
121	122	123	124
125	126	127	128
129	130	131	132
133	134	135	136
137	138	139	140
141	142	143	144
145	146	147	148
149	150	151	152
153	154	155	156
157	158	159	160
161	162	163	164
165	166	167	168
169	170	171	172
173	174	175	176
177	178	179	180
181	182	183	184
185	186	187	188
189	190	191	192
193	194	195	196
197	198	199	200
201	202	203	204
205	206	207	208
209	210	211	212
213	214	215	216
217	218	219	220
221	222	223	224
225	226	227	228
229	230	231	232
233	234	235	236
237	238	239	240
241	242	243	244
245	246	247	248
249	250	251	252
253	254	255	256
257	258	259	260
261	262	263	264
265	266	267	268
269	270	271	272
273	274	275	276
277	278	279	280
281	282	283	284
285	286	287	288
289	290	291	292
293	294	295	296
297	298	299	300
301	302	303	304
305	306	307	308
309	310	311	312
313	314	315	316
317	318	319	320
321	322	323	324
325	326	327	328
329	330	331	332
333	334	335	336
337	338	339	340
341	342	343	344
345	346	347	348
349	350	351	352
353	354	355	356
357	358	359	360
361	362	363	364
365	366	367	368
369	370	371	372
373	374	375	376
377	378	379	380
381	382	383	384
385	386	387	388
389	390	391	392
393	394	395	396
397	398	399	400
401	402	403	404
405	406	407	408
409	410	411	412
413	414	415	416
417	418	419	420
421	422	423	424
425	426	427	428
429	430	431	432
433	434	435	436
437	438	439	440
441	442	443	444
445	446	447	448
449	450	451	452
453	454	455	456
457	458	459	460
461	462	463	464
465	466	467	468
469	470	471	472
473	474	475	476
477	478	479	480
481	482	483	484
485	486	487	488
489	490	491	492
493	494	495	496
497	498	499	500
501	502	503	504
505	506	507	508
509	510	511	512
513	514	515	516
517	518	519	520
521	522	523	524
525	526	527	528
529	530	531	532
533	534	535	536
537	538	539	540
541	542	543	544
545	546	547	548
549	550	551	552
553	554	555	556
557	558	559	560
561	562	563	564
565	566	567	568
569	570	571	572
573	574	575	576
577	578	579	580
581	582	583	584
585	586	587	588
589	590	591	592
593	594	595	596
597	598	599	600
601	602	603	604
605	606	607	608
609	610	611	612
613	614	615	616
617	618	619	620
621	622	623	624
625	626	627	628
629	630	631	632
633	634	635	636
637	638	639	640
641	642	643	644
645	646	647	648
649	650	651	652
653	654	655	656
657	658	659	660
661	662	663	664
665	666	667	668
669	670	671	672
673	674	675	676
677	678	679	680
681	682	683	684
685	686	687	688
689	690	691	692
693	694	695	696
697	698	699	700
701	702	703	704
705	706	707	708
709	710	711	712
713	714	715	716
717	718	719	720
721	722	723	724
725	726	727	728
729	730	731	732
733	734	735	736
737	738	739	740
741	742	743	744
745	746	747	748
749	750	751	752
753	754	755	756
757	758	759	760
761	762	763	764
765	766	767	768
769	770	771	772
773	774	775	776
777	778	779	780
781	782	783	784
785	786	787	788
789	790	791	792
793	794	795	796
797	798	799	800
801	802	803	804
805	806	807	808
809	810	811	812
813	814	815	816
817	818	819	820
821	822	823	824
825	826	827	828
829	830	831	832
833	834	835	836
837	838	839	840
841	842	843	844
845	846	847	848
849	850	851	852
853	854	855	856
857	858	859	860
861	862	863	864
865	866	867	868
869	870	871	872
873	874	875	876
877	878	879	880
881	882	883	884
885	886	887	888
889	890	891	892
893	894	895	896
897	898	899	900
901	902	903	904
905	906	907	908
909	910	911	912
913	914	915	916
917	918	919	920
921	922	923	924
925	926	927	928
929	930	931	932
933	934	935	936
937	938	939	940
941	942	943	944
945	946	947	948
949	950	951	952
953	954	955	956
957	958	959	960
961	962	963	964
965	966	967	968
969	970	971	972
973	974	975	976
977	978	979	980
981	982	983	984
985	986	987	988
989	990	991	992
993	994	995	996
997	998	999	1000

StrataCom Group 2	Rev. 3.0	Oct 21 1987 11:22 PST
Most recent log entries, most recent first		
Class	Description	Size
Class	Removal 12:31	132
Class	Ver. VCD found	80
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11
Info	Control line alarm	11

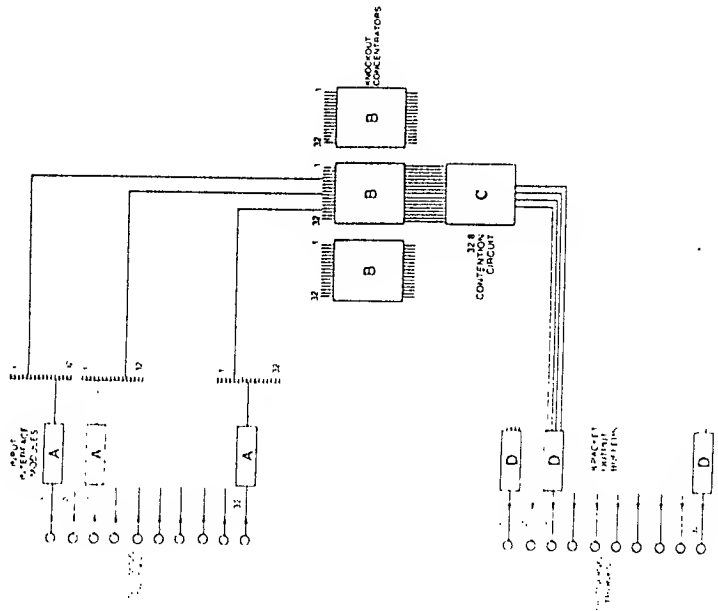


Fig. 22 Knockout II switch—overall block diagram.

until a single final winner results. All others are knocked out. This is a way of sorting on a two-at-a-time basis. This 2×2 organized switch is the heart of this class of switch. We shall later consider its extension into even higher switching speeds.

Since it is unlikely that all packets will be addressed to the same output node, hardware is saved by taking advantage of statistics—concentrate the N packet lines into L output packet buffers. This is shown in Fig. 25. A key design

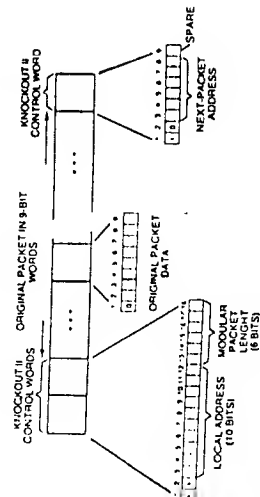


Fig. 23. New packet format at input to the knockout II. (Reference 15, p. 1429.)

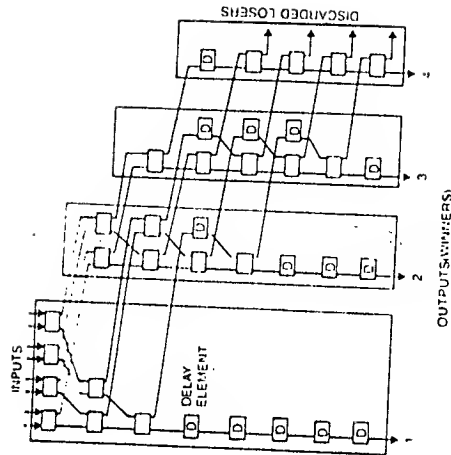


Fig. 24. 8-4 Knockout concentrator. (Reference 15, p. 1434.)

issue in a packet switch is how to handle many packets addressed to the same outgoing link. To avoid packet loss, the packets are buffered. It can be shown that the delay time is appreciably greater if the buffering is done at the input of the switch rather than at the output. Thus the Knockout II approach does all its buffering on its output unit.

In Fig. 26 the first eight winners are seen buffered in the output stack. Conventional computer random-access memory (RAM) is used for the output buffers. The knockout approach guarantees first-in-first-out, and the delay through the switch can be kept very short. Even at 1024 bits per packet, the 32×32 switch can handle 1,375,000 packets per second.

Figure 27 shows that only eight output buffers for a 32×32 switch can essentially prevent any loss of packets. However, this estimate is based upon the

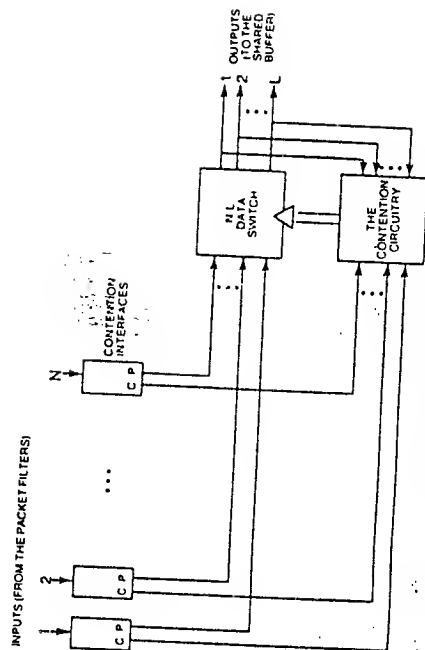


Fig. 25. The $N:L$ concentrator. (Reference 15, p. 1431.)

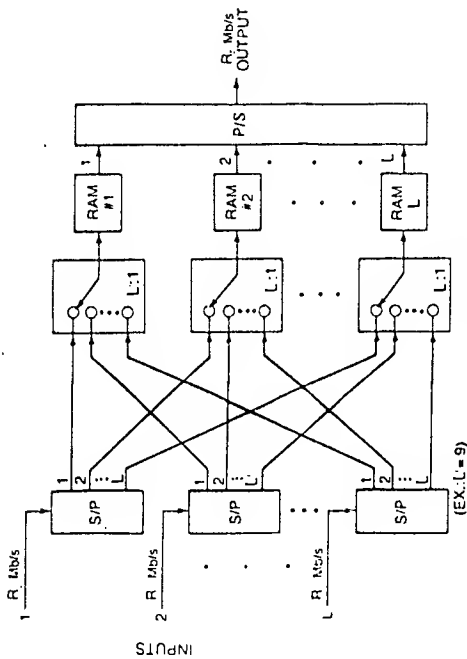


Fig. 26. The shared buffer using RAMs. (Reference 15, p. 1433.)

author's assumption that the traffic is uniformly generated and addressed.

7.3. Some Comparisons

The conventional voice band data-rate packet switches operate from the 100 to 1000 packets per second, or about a 100,000- to 1-Mbps throughput rate. Fast packet voice/data switches tend to run on the order of magnitude of about 24,000 (1024-bit equivalent rate) packets, or a 24-Mbps throughput rate, whereas the early 32×32 knockout II switch operates at about 1,000,000 packet per second, or 32×44 Mbps or 1.4 Gbps.

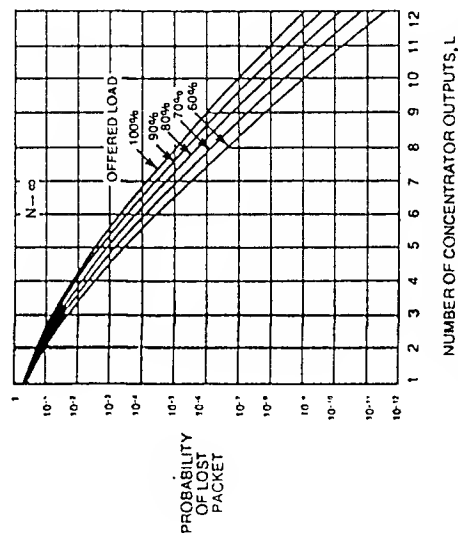


Fig. 27. Lost packet performance concentrator. (Reference 15, p. 1430.)

Even faster speeds are possible and are expected in the future as the packet-handling process evolves toward a stream processing approach using 2×2 switches, rather than as a conventional computer batchlike process. In doing so, the previous sharp difference between packet switching and circuit switching become even fuzzier.

8. Evolution

Conventional digital circuit switches use a combination of space division and time division sections. With increasing data rates, the optimal mix moves to a greater portion of time division and less of space division switching. In very high data rate circuits such as optic fiber, the fibers themselves are heavily time division multiplexed. Since more traffic from different sources is being time-shared over the same digital link, fewer switched lines tend to be needed because more multiplexing and demultiplexing occurs outside of the switch per se. Thus, the future evolving switch topology appears to be that of a fabric of 2×2 hard-wired switches with fewer separate input/output lines. An example of this structure was seen in the illustrative knockout switch case, where packets on each line in the switch fabric are switched with their neighbors in a series-parallel network where all possible permutations are allowed. This is really a hardwired parallel sorting network.

8.1. Batcher-Banyan Networks

One of the slowest operations in a conventional computer is sorting large files. Each item must be compared against all other items, with the examination made serially. To cope with this sort of problem, a distributed form of 2×2 (i.e., two-input, two-output) switch has been well known in the computer art and is called a *Batcher network*. Each pair of items to be compared is input on two input lines. The item with the larger value of the two is connected to output line A while the other input item is sent out on output line B. When each two input sorters are connected in permuted fashion with other similar units, all combinations of inputs are able to reach every output position. This basic structure yields both a very fast sorting engine and a very high speed packet switch simply by controlling the binary switching according to the incoming bit pattern. Such networks are sometimes called *Batcher-banyan networks*, named after K. E. Batcher, who proposed this sorting algorithm in 1969, while the banyan part of the name is attributable to L. Rodney Groke and G. L. Lipovski, who compared the intertwined switching fabric to the East Indian banyan tree with a branching intertwined network of roots.⁽¹⁶⁾ There are a variety of different configurations possible, each with different names (e.g., as shuffle networks). But the details are beyond the scope of this book.

Of most interest to us about the banyan, or shuffle, types of networks is how well they lend themselves to very high data rate input streams, including optical fibers. Optical fiber switches, or *photonic switching*, often described in

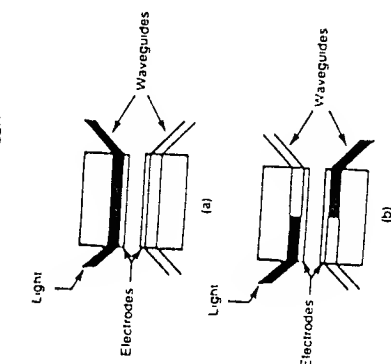


Fig. 28. Optical directional coupler: (a) the straight state of directional coupler, (b) the cross state of a directional coupler. (Reference 14, p. 357.)

the literature but not yet wholly feasible from an engineering standpoint, use electrically controlled directional couplers. In Fig. 28 an applied voltage causes switching the output of the two inputs and two output device, identical to the switching elements of the sorting-banyan-shuffle-type networks previously described. Whether fiber-optic switches evolve to be photonically switched or not is not a major issue, since the switching can be done electrically in the nonoptical domain as well. You might wish to think of these types of switches as a network of train tracks organized on a 2×2 set of crossed tracks. See Fig. 29. The trick is to switch each arriving train to exit on any chosen output track without having the train slow down by utilizing the routing instruction carried by the trains themselves. Each switch exchange requires only one bit of header information. Selecting one out of 1024 output paths would require only 10 routing bits, each sequentially closing its switch at the exact right instant.

Likely network configurations for the future to operate at gigabit per second rates will most likely be organized in shuffle or banyan network configurations, as seen in Fig. 29, and where each packet routes itself through the network.

8.2. Software-Defined Networks

Burger King's slogan is "you get it your way." In the post-AT&T divestiture period, each large communication user is seeking to have its own private overlay network. This is a network composed of leased circuits optimized for the user's needs, thereby eliminating the need to use the public-switched network. These needs evolve and change over time. Some requirements change over the course of a day; more data transmission may be needed at night relative to voice circuits needed during the day. What is increasingly sought is called a *software-defined network*.

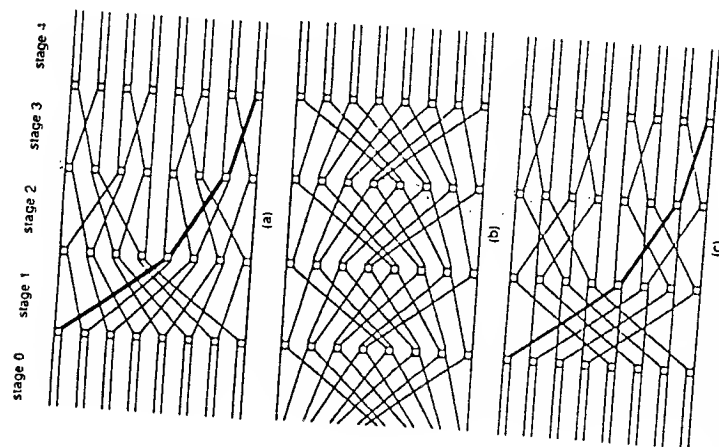


Fig. 29. Shuffle/banyan-type networks. (a) A 16-by-16 baseline network. (b) A 16-by-16 shuffle network. (c) A 16-by-16 banyan network. (Reference 14, p. 356.)

Allowing each customer to have control of its own network configuration in real time by remote computer permits a new freedom of choice to the user, thus creating a more useful and economical network. This growing desire for software-defined networks further combined with the evolution of switching toward all-digital networks is creating another force to increase the portion of the network that is packetized or under packet control.

8.3. The Open Systems Interconnection Protocols

As the packet-switched component of the network increases, the degrees of freedom to the designer become open-ended, allowing extremely complex logical structures to be implemented. It does not take much of this sort of thing to occur before the complexity of what is happening becomes overwhelming. Although communication systems interface standards existed for many years, the explosion of complexity really began with the impact of the wholly software defined computer switch—that is, stored program control switching.

Back in the 1970s the international committees working on packet network interconnection protocol issues came up with a brilliant organizing concept to get their hands around the issues—a hierarchy of protocols, each communicat-

ing only with their higher and lower level protocols. The driving force at that time was the realization that it would be important for computer/packet-switched networks of the world to be able to intercommunicate. To do so, a series of standards would be needed. What was the minimum number of interfaces that had to be standardized and what items should be selected for standardization? This movement, the International Standards Organization Open Systems Interconnection Architecture is now commonly called OSI. OSI is a desire to allow maximum freedom of interconnection of disparate units. This represents a marked change from the earlier days of computers when each manufacturer intentionally attempted to make their system interface unique and proprietary. The last thing that a computer manufacturer wanted was for a competitor to be able to interconnect new units to its system.

The open systems concept is based upon the agreement of a set of international standards that ensure interconnectability with other relevant systems. There is a balance point here. If you try to standardize too many interfaces, you overly limit the freedom for future system improvements, if too few interfaces, then the complexity of the interface specification becomes unwieldy and is again overconstraining. What was chosen was a seven-level hierarchy. See Fig. 30. All communications and computer system functionality can more or less be mapped onto this seven-level hierarchy of aggregation. At the top are protocols that specify what the user wants the system to do. The bottom level defines the lowest level of complexity—where the systems physically tie together, such as the voltages on the signal lines and the connector type. Each layer, starting from the bottom, is numbered, and each layer has been defined as to functions it contains. (This subject is described in great detail in readily available sources and will not be considered here other than to briefly describe what is contained in each layer and to note the importance of these structures in the evolving packet-switching systems of the future.)

Because each protocol speaks *only* to the level above and below, all

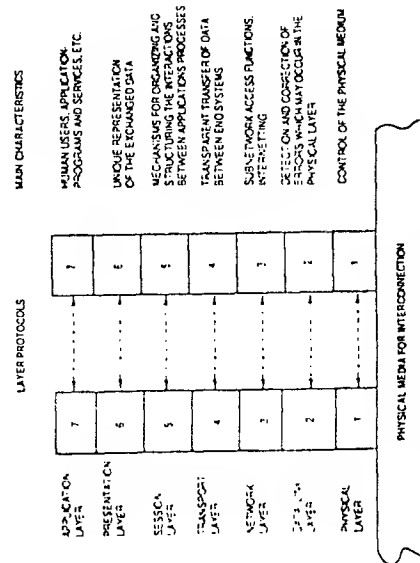


Fig. 30. The seven-layer OSI architecture. (Reference 13.)

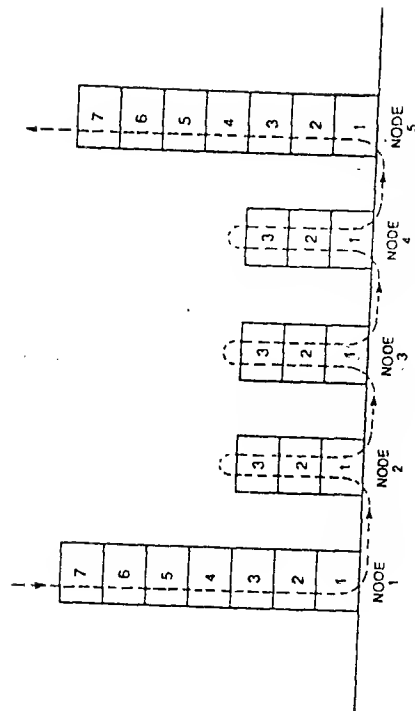


Fig. 31. Path through the hierarchy at each node.

communication between geographically separated sites must go down the hierarchy, move across at the bottom (physical) level, and then up the hierarchy until the desired end point is reached. Figure 31 shows the case of connecting two host computers via three switching nodes. The communication path is shown traversing the protocol layers traversed from an application at one site, packets relayed via three sites and thence to an interacting user at a remote site. Because each protocol level need speak only to the level above and to the level below, the design of each protocol is greatly simplified and can be generalized.

As described earlier in the section on encapsulation, the *data flow between protocol levels is always in the form of packets*. And at each level down the column a new header is appended to the packet, so the data content of the downward moving packets are of no concern to the lower-layer protocols. After the packet is physically transmitted across the physical layer (the "wire" between the two nodes), the headers are stripped off in the upward direction, as shown in Fig. 32. This conceals the internal operation of the system from the user.

The relevance of this essentially all-data-processing functionality to the communications switching process can be seen in Fig. 33. Here we see the protocols used for a circuit-switched configuration in an ISDN system. (ISDN is described in detail in Chapter 12.)

We can see that communication switching in general is now totally melding with the packet-switching art as we move toward a world of all-digital transmission and switching. Analog transmission may be viewed merely as that residual part of the system not yet converted to digital. In the past, digital transmission was synonymous with time division multiplexing, which will likely continue for a while. But encroachment of packet techniques upon the circuit-switched digital network is far along. As described, signaling between switching nodes of the telephone system is already packetized. And with the passage of time the degree of "packetization" is expected to increase further throughout the network.

the network be out of operation when links A, B, C and D are all in operation at the same time? (b) How many hours per year would node E be out of operation because of link failure?

6. Two independent packet networks are to be connected together. The headers of the packets in each system are entirely different.

To address	From address	Sequence Number	Data Field 120b	CRC-16 bit
From address	To address	No sequence length if data field	Variable length Data field	CRC-8 bit

(a) You are asked to build a gateway between these two networks. What functions are required to interconnect into the other? (b) Is this possible? (c) How do you handle the differences in the field, i.e., lack of a sequence number, a variable length data field versus a fixed light field? (d) What ways are there to handle a variable data field with 127 bits when the next system uses bytes, i.e., modulo 8?

7. (a) What are the problems encountered in building very large packet switching networks? (Hint: efficiency, routing table lengths, housekeeping information, etc.)? (b) How might you go about overcoming these constraints? (c) Is there any reason why an infinite size packet switched network cannot be built?

References

1. Data Communications, March 1988, p. 270, glossary compiled by staff of Data Communications.
2. F. A. Tabogi, M. Gerla, R. W. Peebles, and E. G. Manning, "Modeling and Measurement Techniques in Packet Communication Networks," *Proc. IEEE*, vol. 66, no. 11, 1978.
3. P. Baran, "On Distributed Communications," Vols. I-XI, Rand memoranda, August 1964, The Rand Corporation, Santa Monica. Part of work is summarized in "On Distributed Communications Networks," *IEEE Trans. Commun. Syst.*, vol. CS-12, pp. 1-9, 1964.
4. D. W. Davies, K. A. Bartlett, R. A. Scantlebury, and P. T. Wilkinson, "A Digital Communications Network for Computers Giving Rapid Response at Remote Terminals," *Proc. ACM Symp. on Operating System Principles*, Gatlinburg, 1967.
5. L. G. Roberts and B. D. Wessler, "Computer Network Development to Achieve Resource Sharing," *AFIPS Conf. Proc. S.J.C.C.*, vol. 36, p. 543+, 1970.
6. N. Abrahamson, "The ALOHA System—Another Alternative for Computer Communications," *FJCC Conf. Proc.*, vol. 37, AFIPS Press, pp. 281-85, 1970.
7. R. Kahn, "The Organization of Computer Resources into a Packet Radio Network," *IEEE Trans. Commun.*, Jan. 1977.

Packet Switching

8. S. Fraleigh and J. Garrett, "A Technology for Packet Radio," *AFIPS Conf. Proc.*, vol. 44, 1975.
9. N. Abrahamson, "Packet Switching with Satellites," *AFIPS Conf. Proc.*, vol. 42, pp. 695-702, 1973.
10. L. G. Roberts, "ALOHA Packet Systems with and Without Slots and Capture," *Satellite Systems Note 8 (NIC 11290)* June 1972, reprinted in *Computer Comm. Rev.*, vol. 5, 1975.
11. R. M. Metcalfe and D. R. Boggs, "Ethernet: Distributed Packet Switching for Local Computer Networks," *Comm. ACM*, vol. 19, pp. 395-404, 1976.
12. W. Stallings, "Handbook of Computer Communications Standards," vol. 1, The open systems interconnection (OSI) model and OSI-Related standards, Macmillan, New York, 1987, pp. 3-4.
13. P. J. Kuen, in *ISDN-Technology, Networking Concepts and Applications*, from Lecture Notes in Computer Science, No. 248, Networking in Open Systems, Gunter Muller and Robert P. Blanc, eds., 1986, p. 88.
14. B. N. W. Ma and J. W. Mark, "Performance Analysis of Burst Switching for Integrated Voice/Data Services," *IEEE Trans.*, vol. 36, No. 3, p. 282, 1988.
15. Kai Y. Eng, M. G. Hluchyj, and Yu-Shuan Yeh, "A Knockout Switch for Variable-Length Packets," *IEEE J. Selected Areas Commun.*, vol. SAC-5, no. 9, p. 1426, 1987.
16. P. Bors, "Self Sorting Networks May Help Switches Catch Up to Signal Speeds," *Data Commun.*, Dec. pp. 68-70, 1987.

RELIABLE DIGITAL COMMUNICATIONS SYSTEMS
USING UNRELIABLE NETWORK REPEATER NODES

Paul Baran
➤ Mathematics Division
The RAND Corporation

P-1995

May 27, 1960

Reproduced by

The RAND Corporation • Santa Monica • California

The views expressed in this paper are not necessarily those of the Corporation

RELIABLE DIGITAL COMMUNICATIONS SYSTEMS
UTILIZING UNRELIABLE NETWORK REPEATER NODES

INTRODUCTION

The cloud-of-doom attitude that nuclear war spells the end of the earth is slowly lifting from the minds of the many. Better quantitative estimates of post-attack destruction together with a less emotional discussion of the alternatives may mark the end of the "what the hell--what's the use?" era. A new view emerges: the possibility of a war exists but there is much that can be done to minimize the consequences.

If war does not mean the end of the earth in a black and white manner, then it follows that we should do those things that make the shade of grey as light as possible: to plan now to minimize potential destruction and to do all those things necessary to permit the survivors of the holocaust to shuck their ashes and reconstruct the economy swiftly.

PURPOSE

This paper is directed toward the communications system designer in the hope that he will not neglect these problems of survival in the design of his future systems. Unfortunately, no panacea can be presented.

There is none. Only a single limited technique is described, that of using one form of distributed redundancy to minimize vulnerability. A detailed examination demonstrates that the problem is not an unsolvable one, but that much money and much work are necessary to provide all the elements needed for the true solution to the vulnerability problem.

The timing for such thinking is particularly appropriate now. for we are just beginning to design and lay out designs for the digital data transmission systems of the future. We are just approaching the initiation state of the designs of systems where computers speak to one another. When this day comes, the digital communications system capacity needed will be orders of magnitude greater than our chief present-day digital transmission technique; namely, teletype. For example, a 60 WPM teletype channel would take about two weeks, operating 24 hours per day without breakdown, to transmit a single standard size reel of magnetic tape used on a digital computer. This may be compared to a writing time of about 6 minutes on the computer.

Time is right.

Millimicrosecond clock rate data links will be needed in the future. Our present communications plant will not suffice. As there does not seem to be any fundamental technical problem that prohibits the operation of digital communications links at the clock rate of digital computers, the view is taken that it is only a matter of time before such design requirements become hardware. The systems designs of the next few years will be the systems-in-being of the next few decades. It is hoped

that these systems will be foresighted enough to include an insurance policy purchasing invulnerability.

CONTENTS

This first paper of this series describes a rationale for the use of redundancy in networks and the payoff for varying degrees of such redundancy.

The second paper, by Frank Yates and Paul Baran, describes a high speed automatic switching technique for digital messages. In this paper the time of arrival of messages is used to determine the shortest routing paths over a severely damaged network.

The third paper, by Paul Baran and Robert Hamerly, describes a lower speed digital system using a tag containing the number of times a message has been relayed to provide a method for authenticating point of origin.

These two separate systems exhibit different properties; it is possible to multiplex them together to utilize the advantages of both and devise a third system. It is thus possible to visualize a new set of systems based upon a distributed organization.

Automatic route selection is not new, but these papers seek as a common goal synthesis of systems where the intelligence required to switch signals to surviving links is at the link nodes and not at one or a few centralized switching centers. This paper thus describes what we choose to call distributed organization as compared to the more familiar centralized switching center type organization.

IEEE publications

scanning the issues
advance abstracts
translated journals
special publications

Scanning the issues

Distributed Communications. A great deal of thought has necessarily been given in recent years to the question of the survivability of communications systems in the event of attack. Unpleasant though such a prospect may be, the studies themselves have led to some interesting suggestions as to what form our future networks might take.

Of particular interest is the distributed communication network concept in which each station is connected to all adjacent stations rather than to a few switching points, as in a centralized system.

Although one can draw a wide variety of networks, they all factor into two components: centralized (or star) and distributed (or grid or mesh). (See types (A) and (C), respectively in Fig. 1.)

The centralized network is obviously

vulnerable, as destruction of a single central node destroys communication between the end stations. In practice, a mixture of star and mesh components is used to form communications networks. For example, type (B) in Fig. 1 shows the hierarchical structure of a set of stars connected in the form of a larger star with an additional link forming a loop. Such a network is sometimes called a "decentralized" network, because complete reliance upon a single point is not always required.

Since destruction of a small number of nodes in a decentralized network can destroy communications, the properties, problems, and hopes of building "distributed" communications networks are of paramount interest.

In a recent study of the effects of an attack on a distributed network, an investigation was made of the percentage of surviving linked stations versus the probability of station destruction for various levels of network redundancy. Redundancy level is a measure of connectivity and is used here as defined in Fig. 2.

A key point revealed by the study is that extremely survivable networks can be built with the use of a moderately low redundancy of connectivity level. Redundancy levels on the order of only three permit the withstanding of extremely heavy level attacks with negligible additional communications loss.

In addition, when one studies what happens when the links rather than the nodes of the network are destroyed, it becomes evident that highly reliable networks can be achieved with low-cost unreliable communication links, even links so unreliable as to be unusable in present networks.

Our future systems design problem is that of building at lowest cost very reliable systems out of the described set of unreliable elements. For communications of the future, digital links appear increasingly attractive by permitting low-cost switching and low-cost links.

In any event the network must be built with the expectation of heavy damage. Powerful error removal methods exist.

Some of the communication construction methods that look attractive for the near future include pulse regenerative repeater line, minimum-cost or "minicost" microwave, TV broadcast station digital transmission, and satellites.

In communications, as in transporta-

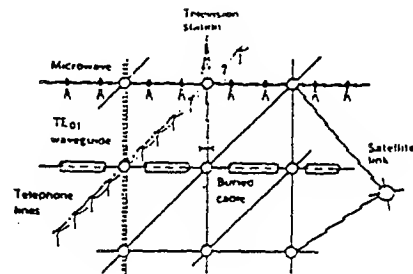


Fig. 3. All-digital network composed of mixture of links.

tion, it is most economical for many users to share a common resource rather than for each to build his own system, particularly when intermittent or occasional service is supplied. This intermittency of service is highly characteristic of digital communication requirements. Therefore, we would like to consider one day the interconnection of many all-digital links to provide a resource optimized for the handling of data for many potential intermittent users: a new common-user system.

Fig. 3 demonstrates the basic notion: A wide mixture of different digital transmission links is combined to form a common resource divided among many potential users. (P. Baran, "On Distributed Communications Networks," *IEEE Trans. on Communications Systems*, March 1964.)

Repetition in Learning. Learning is facilitated when subject matter is presented in extremely small segments and the student is stimulated to respond immediately, at frequent but increasingly

Fig. 1. (A) Centralized. (B) Decentralized. (C) Distribution networks.

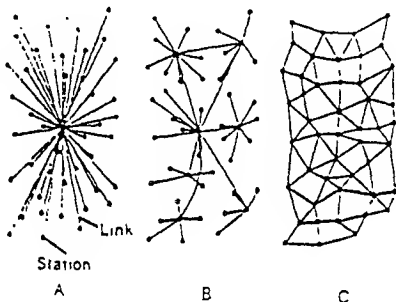
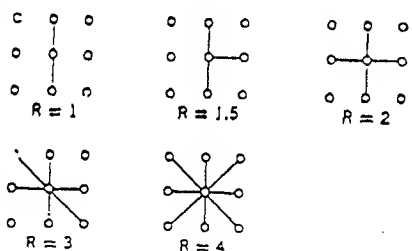


Fig. 2. Definition of redundancy level.



SUBSCRIBERS TO RAND RESEARCH PUBLICATIONS

Some 290 libraries, research centers, and businesses around the world are subscribers to RAND publications.

Subscriptions are provided by the Corporation on a calendar year basis.

The RAND publications in most libraries are available to library patrons on the same basis as other holdings and are subject to the same rules and

regulations. They may be obtained by patrons of other libraries through the Interlibrary Loan Service. Subscriber libraries are authorized to reproduce materials from the RAND collection for their patrons.

Each subscriber listed below has accumulated annual collections of unclassified RAND publications beginning with the year indicated in parentheses

Subscribers in the United States

ALABAMA

Auburn University, Ralph Brown Draughon Library (1965)
JETS/ISAC Library (1987)
Samford University, Law Library (1989)
University of Alabama in Birmingham, Mervyn H. Sterne Library (1985)
Jacksonville State University, Cole Library (1973)
University of Alabama Library (1971)

ARIZONA

Tempe
Tucson
University of Arizona, College of Law Library (1989)
University of Arizona Library (1965)

ARKANSAS

Fayetteville
Little Rock
University of Arkansas Library (1970)
Arkansas State Library (1983)

CALIFORNIA

Bakersfield
Berkeley
Carson
Chico
Cypress
Davis
Domínguez Hills
Fullerton
Inglewood
Irvine
La Jolla
Long Beach
Los Angeles
Los Angeles
Malibu
Monterey
Pasadena
Pomona
California State College Library (1972)
University of California, Main Library (1953)
Atlas Airfreight System (1986)
Chico State University Library (1963)
PacifiCare (1989)
University of California Library (1969)
California State College Library (1972)
California State University Library (1968)
Inglewood Public Library (1989)
University of California, General Library (1965)
Long Beach Public Library (1989)
University of California Library (1972)
Aerospace Corporation (1975)
University of California, University Research Library (1953)
University of Southern California, Doheny Library (1965)
Pepperdine University, Payson Library (1989)
Naval Postgraduate School Library (1972)
California Institute of Technology, General Library (1953)
California State Polytechnic University Library (1968)

Redondo Beach
Riverside

Robert Park
Sacramento
San Diego
San Francisco
San Francisco
Santa Barbara
Santa Clara
Santa Cruz
Santa Monica
Stanford
TRW Technical Information Center (1974)
University of California Library (1967-1982, 1986)
California State College Library, Sonoma (1970)
California State Library (1969)
California State University Library (1972)
San Diego State University, Malcolm A. Love Library (1973)
Golden Gate University, General Library (1977)
USSR Consulate General, Library (1989)
University of California, Sciences-Engineering Library (1968)
University of Santa Clara, Orredine Library (1971)
University of California Library (1989)
Santa Monica Public Library (1982)
Stanford University, Green Library (1953)

COLORADO

Boulder
Colorado Springs
Denver
Denver
Fort Collins
University of Colorado Libraries (1977)
U.S. Air Force Academy, Hq USAFA/DFSEL (1968)
Denver Public Library (1953)
University of Denver, Penrose Library (1973)
Colorado State University Libraries (1973)

CONNECTICUT

Hartford
Middletown
New Haven
Storrs
Connecticut State Library (1980)
Wesleyan University, Olin Library (1970)
Yale University Library (1953)
University of Connecticut, Homer Babbidge Library (1963)

DELAWARE

Newark
University of Delaware, Morris Library (1972)

FLORIDA

Coral Gables
Gainesville
Miami
Tallahassee
Tampa
University of Miami Library (1967)
University of Florida Libraries (1984)
Florida International University Library (1972)
Florida State University Library (1972)
University of South Florida Library (1970)

GEORGIA

Athens
Atlanta
Atlanta
University of Georgia Libraries (1967)
Georgia Institute of Technology, Price Gilbert Library (1953)
Georgia State University Library (1972)

HAWAII

Honolulu
University of Hawaii Library (1953)

ILLINOIS

Carbondale
Charleston
Chicago
Chicago
Chicago
DeKalb
Evanston
Macomb
Rosemont
Springfield
Southern Illinois University, Morris Library (1975)
Eastern Illinois University, Booth Library (1963)
Chicago Public Library (1973)
University of Chicago Library (1953)
University of Illinois at Chicago Circle, Library (1974)
Northern Illinois University, Founders Memorial Library (1964)
Northern Illinois University Library (1969)
Western Illinois University Library (1974)
WEB America (1986)
Illinois State Library (1972)

- Springfield
Urbana
- INDIANA
Bloomington
Indiana State University (1988)
Indiana University-Purdue University (1971)
Lafayette
Notre Dame
- IOWA
Ames
Des Moines
Iowa City
- KANSAS
Lawrence
Manhattan
Wichita
- KENTUCKY
Bowling Green
Lexington
- LOUISIANA
Baton Rouge
Baton Rouge
New Orleans
New Orleans
- MARYLAND
Baltimore
College Park
- MASSACHUSETTS
Amherst
Boston
Boston
Boston
Cambridge
Cambridge
Chestnut Hill
North Easton
Springfield
- MICHIGAN
Ann Arbor
Detroit
Detroit
East Lansing
Farmington Hills
Kalamazoo
Lansing
Ypsilanti
- Sagamore State University Library (1966)
University of Illinois Library (1953)
- Indiana University Library (1966)
Butler University Library (1988)
Hudson Institute Library (1986)
Indiana University-Purdue University (1971)
Purdue University Library (1963)
University of Notre Dame, Memorial Library (1970)
- Iowa State University, Parks Library (1953)
Drake University Library (1981)
University of Iowa Libraries (1953)
- University of Kansas Libraries (1970)
Kansas State University, Farrell Library (1965)
Wichita State University Library (1970)
- Western Kentucky University, Helm-Cravens Library (1973)
University of Kentucky Library (1953)
- Louisiana State University Library (1983)
Southern University Library (1972)
Tulane University Library (1965)
U.S. Courts Library (1989)
- Johns Hopkins University, Milton S. Eisenhower Library (1953)
University of Maryland, Engineering Library (1966)
- University of Massachusetts Library (1967)
Boston Public Library (1965)
Boston University Libraries (1982)
Northeastern University Libraries (1975)
Kennedy School of Government (1981)
Massachusetts Institute of Technology Libraries (1953)
Boston College, O'Neil Library (1965)
Stonehill College, Cushing-Martin Library (1989)
Western New England College, Churchill Library (1980)
- University of Michigan Library (1953)
Detroit Public Library, Technology and Science Department (1966)
Wayne State University, Arthur Neef Law Library (1989)
Michigan State University Library (1965)
Oakland Community College Library (1989)
Western Michigan University, Dwight B. Waldo Library (1965)
Library of Michigan (1974)
Eastern Michigan University Library (1971)
- MINNESOTA
Minneapolis
Minneapolis
Northfield
- MISSISSIPPI
University
- MISSOURI
Columbia
Kirksville
St. Louis
St. Louis
- NEBRASKA
Lincoln
Omaha
- NEVADA
Las Vegas
Reno
- NEW HAMPSHIRE
Durham
Hanover
- NEW JERSEY
Glasboro
Newark
New Brunswick
Princeton
Trenton
- NEW MEXICO
Albuquerque
- NEW YORK
Albany
Albany
Bethpage
Binghamton
Buffalo
Canton
Ithaca
New Rochelle
New York
New York
New York
New York
New York
APO New York
- Rochester
Stony Brook
Syracuse
- Minneapolis Public Library (1971)
University of Minnesota Libraries (1953)
Carleton College Library (1984)
- University of Mississippi, John Davis Williams Library (1972)
- University of Missouri Library (1965)
Northeast Missouri State University, Pickler Library (1970)
University of Missouri at St. Louis, Thomas Jefferson Library (1964)
Washington University Libraries (1953)
- University of Nebraska Libraries (1953)
University of Nebraska at Omaha, University Library (1979)
- University of Nevada Library (1966)
University of Nevada Library (1967)
- University of New Hampshire Library (1971)
Dartmouth College, Baker Library (1968)
- Glasboro State College, Savitz Library (1981)
Newark Public Library (1972)
Ruigers University, Alexander Library (1978)
Princeton University Library (1953)
Trenton State College Library (1969)
- University of New Mexico, General Library (1968)
- New York State Library (1968)
State University of New York at Albany, Library (1970)
Gruman Services Divisions (1971)
State University of New York at Binghamton, Library (1971)
Buffalo & Erie County Public Library (1963)
St. Lawrence University Library (1969)
Cornell University Library (1953)
Iona College, Ryan Library (1973)
ABC News Research Center (1989)
Columbia University Libraries (1953)
New York Public Library (1953)
Public Affairs Information Service, Inc. (1989)
The Rockefeller University Library (1979)
Hq. U.S. Army Europe & 7th Army (AEAG-ALU), Library and Resource Center (1985)
University of Rochester Library (1969)
State University of New York at Stony Brook Library (1965)
Syracuse University Library (1965)

- Utica
State University of New York at Utica. College of Technology Library (1970)
- NORTH CAROLINA**
Chapel Hill
Duke University Library (1953)
Greensboro
University of North Carolina at Greensboro. Library (1972)
Raleigh
North Carolina State University. D. H. Hill Library (1973)
- OHIO**
Cincinnati
Public Library of Cincinnati (1969)
Cincinnati
University of Cincinnati. Main Campus Library (1969)
Cleveland
Case Western Reserve University. Sears Library (1965)
Cleveland
Cleveland Public Library (1953)
Columbus
Cleveland State University Library (1977)
Dayton
Ohio State University Libraries (1953)
Kent
Air Force Institute of Technology Library (1967)
Oxford
Kent State University Library (1963)
Toledo
Miami University Libraries (1971)
University of Toledo Library (1970)
- OKLAHOMA**
Norman
University of Oklahoma Library (1953)
Tahlequah
Northeastern Oklahoma State University Library (1972)
Tulsa
University of Tulsa. McFarlin Library (1973)
- OREGON**
Portland
Portland State University Library (1970)
Salem
Oregon State Library (1970)
Salem
Willamette University Library (1989)
- PENNSYLVANIA**
Collegeville
Ursinus College Library (1989)
Indiana
Indiana University of Pennsylvania Library (1983)
Philadelphia
Drexel University Library (1971)
Philadelphia
Temple University Library (1970)
Pittsburgh
University of Pittsburgh. Hillman Library (1968)
Swarthmore
Swarthmore College Library (1976)
University Park
Pennsylvania State University. Pattee Library (1965)
- RHODE ISLAND**
Providence
Brown University Library (1953)
- SOUTH CAROLINA**
Clemson
Clemson University Library (1973)
Columbia
University of South Carolina. Thomas Cooper Library (1969)
- TENNESSEE**
Chattanooga
University of Tennessee Library (1974)
Cookeville
Tennessee Tech University Library (1982)
Johnson City
East Tennessee State University Library (1974)
Knoxville
University of Tennessee Library (1972)
Memphis
Memphis State University Library (1964)
Nashville
Vanderbilt University Library (1953)
- TEXAS**
Austin
University of Texas. General Library (1953)
College Station
Texas A&M University Library (1965)
Dallas
Dallas Public Library (1980)
Dallas
Southern Methodist University. Underwood Law Library (1989)
Houston
Rice University Library (1958)
Houston
University of Texas. Health Science Center at Houston (1989)
Lubbock
Texas Tech University Library (1969)
San Antonio
Trinity University Library (1974)
San Marcos
Southwest Texas State University Library (1982)
Waco
Baylor University. Memorial Library (1981)
- UTAH**
Provo
Brigham Young University Library (1965)
Salt Lake City
University of Utah. Marriott Library (1953-1971, 1973)
- VERMONT**
Burlington
University of Vermont Library (1978)
- VIRGINIA**
Blacksburg
Virginia Polytechnic Institute and State University Library (1965)
Charlottesville
University of Virginia. Alderman Library (1953)
Charlottesville
University of Virginia. Arthur J. Morris Law Library (1984)
Fairfax
George Mason University Library (1979)
Richmond
University of Richmond. Boatwright Memorial Library (1974)
Richmond
Virginia Commonwealth University. James Branch Cabell Library (1975)
- WASHINGTON**
Olympia
Washington State Library (1970)
Pullman
Washington State University Library (1967)
Seattle
The Boeing Company. Renton Technical Library (1966)
Seattle
University of Washington Libraries (1953)
- WISCONSIN**
DePere
St. Norbert College. Todd Wehr Library (1989)
Green Bay
University of Wisconsin-Green Bay Library (1967)
Madison
University of Wisconsin. Memorial Library (1953)
Milwaukee
Milwaukee Public Library (1971)
Milwaukee
University of Wisconsin-Milwaukee Library (1972)
- DISTRICT OF COLUMBIA**
Washington
Georgetown University Library (1984)
Washington
George Washington University Library (1970)
Washington
Library of Congress (1953)
Washington
National Defense University (1984)
Washington
The Pentagon Library (1970)
Washington
Turkish Embassy (1986)
- PUERTO RICO**
Rio Piedras
Universidad de Puerto Rico. Biblioteca General (1966)

Subscribers in Other Countries.

AUSTRALIA

Brisbane, Queensland
Bundoora, Victoria
Canberra, A.C.T.
Canberra, A.C.T.
Canberra, A.C.T.
Nedlands, W.A.
Sydney, N.S.W.

BELGIUM

Bibliotek Voor Hedendaagse Documentatie (1975)

CANADA

Burnaby, B.C.
Calgary, Alberta
Fredericton, N.B.
Guelph, Ontario
Halifax, N.S.
Hamilton, Ontario
London, Ontario
Montreal, Quebec
Ottawa, Ontario
Ottawa, Ontario
Ottawa, Ontario
Ottawa, Ontario
Toronto, Ontario
Vancouver, B.C.
Windsor, Ontario
Winnipeg, Manitoba

CHINA, REPUBLIC OF

Taipei, Taiwan
Taipei, Taiwan

DENMARK

Aarhus C

ENGLAND

Boston Spa, Yorkshire
London
Oxford

FRANCE

Paris Armees

GERMANY (WEST)

Berlin
Berlin-Charlottenburg
Bonn
Göttingen
Hamburg
Hannover, Welfengarten

Kiel

Kiel
Köln
Konstanz
Münch

INDIA

New Delhi
New Delhi
New Delhi
New Delhi

INDONESIA

Djakarta
Centre for Strategic and International Studies (1972)

ISRAEL

Tel-Aviv
Tel-Aviv University, Library of Social Sciences and Management (1965)

JAPAN

Kamakura, Kanagawa
Tokyo
Tokyo
National Diet Library (1958)

KOREA

Daejeon
Seoul
Seoul
Seoul
Agency for Defense Development, Technical Library (1980)
Institute for Communications Research, Library (1985)
Korea Institute for Defense Analyses, Library (1981)
Korea Social Science Research Library (1982)
The Research Institute for International Affairs, Library (1981)

KUWAIT

Kuwait
Kuwait University Library (1975)

MALAYSIA

Bangi, Selangor
Kuala Lumpur
Universiti Kebangsaan Malaysia, Library (1971)
University of Malaysia Library (1974)

MEXICO

Puebla, Puebla
Universidad de las Americas, Learning Resources Center Library (1972)

THE NETHERLANDS

Delft
Technological University Library (1972)

NEW ZEALAND

Wellington
General Assembly Library (1971)

NORWAY

Trondheim
The Technical University, Library of Norway (1971)

SAUDI ARABIA

Riyadh
Arabian Data Systems (1988)

SCOTLAND

Aberdeen
Aberdeen University Library, Queen Mother Library (1973)

AUSTRALIA

Brisbane, Queensland (1973)
La Trobe University Library (1971)
Australian National University Library (Menzies) (1968)
Department of Defence, Defence Central Library (1978)
National Library of Australia (1969)
University of Western Australia Library (1973)
University of Sydney, Fisher Library (1958)

BELGIUM

Bibliotek Voor Hedendaagse Documentatie (1975)

CANADA

Simon Fraser University, Bennett Library (1970)
University of Calgary Library (1973)
University of New Brunswick, Harriet Irving Library (1969)
University of Guelph Library (1968)
Dalhousie University Library (1968)
McMaster University, Mills Memorial Library (1968)
University of Western Ontario Library (1977)
McGill University Library (1968)
Carleton University Library (1968)
CSIS, Information Centre (1984)
National Defence HQ, Ozee Library (1989)
National Research Council Library (1958)
University of Toronto Library (1966)
University of British Columbia Library (1970)
University of Windsor Library (1970)
University of Manitoba, Elizabeth Dafoe Library (1973)

CHINA, REPUBLIC OF

Institute of American Culture, Academia Sinica (1987)
Tamkang University, Sheng Memorial Library (1970)

DENMARK

Statistikbibliotek, Universitetsparken (1972)

ENGLAND

British Library (1958)
Ministry of Defence Library (1967)
Institute of Economics and Statistics (1971)

FRANCE

Bibliothèque Centrale Cedoc (1986)

GERMANY (WEST)

Preussischer Kulturbesitz, Staatsbibliothek (1971)
Universitätsbibliothek der Technischen Universität Berlin (1969)
Deutscher Bundestag Bibliothek (1973)
Niedersächsische Staats- und Universitätsbibliothek Göttingen (1970)
Staats- und Universitätsbibliothek (1971)
Universitätsbibliothek Hannover und Technische Informationsbibliothek (1968)

SOUTH AFRICA	
Pretoria, Transvaal	Universiteit van Pretoria, Merensky-Biblioteek (1971)
SPAIN	
Madrid	Instituto de Cuestiones Internacionales Library (1982)
SWEDEN	
Nyköping	Studsvik Energietechnik AB (1958)
SWITZERLAND	
Zürich	ETH-Bibliothek (1969)

THE RAND CORPORATION 1989

1700 Main Street, P.O. Box 2138, Santa Monica, California 90406-2138
 2100 M Street, N.W., Washington, D.C. 20037-1270